Analysis of an Incentives-Based Secrets Protection System

N. Boris Margolin Matthew K. Wright Brian N. Levine
Department of Computer Science
University of Massachusetts, Amherst, MA 01003
{margolin,mwright,brian}@cs.umass.edu

ABSTRACT

Once electronic content has been released it is very difficult to prevent copies of the content from being widely distributed. Such distribution can cause economic harm to the content's copyright owner and others. Our protocol, SPIES, allows one party to sell a secret to second party and provides an economic incentive for two parties to limit sharing of a secret between themselves. We do not use watermarking or traditional DRM mechanisms. We focus on content which is to be shared between two parties only, which is valuable, and which only needs to be protected for a limited amount of time. Examples include passwords to a subscription service, pre-release of media for review, or content shared but bound by a non-disclosure agreement. With SPIES, any possesor of the content can receive a portion of the funds placed in escrow by the two legitimate possesors. We analyze this system and show that the best strategy of the content provider and content consumer to maximize their utility is to use SPIES and not share the content further. We deal successfully with a "dummy registration" attack in which multiple false identities are used in an attempt to get a higher payment. We also discuss how to determine the correct escrow amount.

Categories and Subject Descriptors

J.4 [**Social and Behavioral Sciences**]: Economics

General Terms

Algorithms, Economics, Security

Keywords

Incentives, digital rights management, economics

This work was supported in part by National Science Foundation awards ANI-033055, ANI-0087482, and EIA-0080199A.

DRM'04, October 25, 2004, Washington, DC, USA.

1. INTRODUCTION

Providers of subscription-based digital services or content face a difficult challenge in protecting their offerings. Many providers, including wireless hotspots, online periodicals, and databases, protect access by requiring subscribers to log in with a password. However, once a password is known by the consumer, access to such accounts can easily be given away or shared among a large group of people online. From the provider's perspective, all but one of the users will be accessing the service or content without paying, which represents lost profit.

In this paper, we present a protocol that provides an economic incentive to not share secrets such as passwords for these services. Our protocol, called *Secret Protection Incentive-based Escrow System* (SPIES), is suited for applications where a secret must be protected for only a limited period of time and shared between two parties, usually the provider and consumer of the secret. Although SPIES requires a limited time period, extending the period is possible: a SPIES-supported subscription may easily be renewed each month by the consumer.

In addition to subscription service passwords, our scheme is applicable to several other scenarios where intellectual property is released to an individual or corporation prior to public release. For example, SPIES can provide incentive against sharing for a movie pre-released to a reviewer, against sharing of a new operating system pre-released to a collaborator, or against double-selling of exclusive rights to a photo sold to a magazine for later release.

We do not intend for SPIES to replace terms-of-use policies, non-disclosure agreements, corporate policies and procedures, or other legal, technical, or physical protection layers. Rather, we aim to add economic incentives as an additional layer of protection for systems that already have such safeguards.

SPIES has several stages for each subscription. In first stage, the subscriber places a *security deposit* into an escrow account or bindingly agrees to pay it if the secret (e.g., a password) is shared. The subscriber also pays directly to the provider the cost of the secret, if appropriate. The subscriber then receives access to the secret. The second phase then begins and lasts until the end of a distinct *protection period*. During this period anyone who has a copy of the secret can send a commitment to their content to the escrow service. In the third and final phase, all registrants from the second phase are entitled to receive a portion of the security deposit once they prove they have the protected content.

Therefore, the incentive of the legitimate possessors is not to share the secret least they lose the security deposit.

In this paper, we discuss the details of SPIES and analyze the strategies and economic interests of the participants in the protocol. We further discuss applications, and evaluate attacks on the system and alternatives to the SPIES approach.

A preliminary version of SPIES was presented elsewhere [6], and this paper presents several improvements due to that discussion. First, the application of SPIES to password sharing problems is completely new. We've also detailed a number of other new scenarios in Section 3. Second, we've added a new discussion on how to set the escrow price appropriately, also in Section 3. The analysis of the strategies of the participants in Section 4 is also presented here for the first time. Finally, we've modified the protocol to address a version of the prisoner's dilemma. If there are several authorized possessors, each is more likely to sell the secret if she believes that anyone else is likely to. Although there is still an incentive not to sell, it is weakened by the fear of others sharing the secret. Therefore we have restricted SPIES to situations with only a single authorized possessor beyond the secret provider.

2. RELATED WORK

Horne, Pinkas, and Sander [4] have presented the work most similar to ours. They describe an incentive scheme for controlled sharing using escrow. In contrast to our approach, in theirs users are paid for sharing content with authorized users, rather than for refraining from sharing. The payments motivate authorized users to keep content within a subscription community; this effect is similar to that of our incentives. It differs in that our scheme does not require a subscription community.

Golle, *et al* [3], construct a game-theoretic model of peer-to-peer file sharing and study several incentive schemes to deal with the *free-rider* problem. But again, this scheme provide incentives for sharing, rather than for keeping information private or deterring shared access.

A number of systems have been created to handle digital rights management. For example, Microsoft offers a Windows Media DRM system that aims to keep users who receive streaming content from being able to copy the content from the stream [7]. Unlike DRM systems such as this, SPIES does hide or protect content from the user. SPIES provides a disincentive to sharing *access* to the content. SPIES relies on the user's self-interest to stop more widespread distribution of the access password. However, SPIES can be used in conjunction with almost any DRM system.

SPIES allows possessors of secrets to anonymously contact the escrow service, if they wish. Fortunately, anonymity is a well understood problem, and there are many extant protocols that provide sufficient protection. These include Hordes [5], Onion Routing [9] and Web Mixes [2].

3. SPIES

In this section, we detail the operation of SPIES, which provides incentive for not sharing a secret beyond two parties.

We believe the best application of SPIES is to provide an incentive not to share access to password protected service. For example, SPIES can work for a news or magazine site like salon.com; or access to paid-access to wireless hotspots, as is offered by T-mobile at Starbucks cafes. This is the application described in this section. After presenting a formal description of SPIES, we discuss how SPIES can be used to protect against sharing of content other than passwords.

SPIES operates in three distinct phases.

1. During the *Exchange* phase, the consumer places a certain sum of money at risk, either by depositing it in an escrow account or by agreeing to be liable for that sum in the event of secret sharing. Next she receives a password that allows access to the protected service or content. The provider of the password also places a sum of money at risk.

2. During the *Registration* phase anyone in the general public can provide proof of knowledge of the password to an escrow service. This can be the password itself or a cryptographic hash of the secret.

3. During the *Payment* phase all who provided proof in the Registration phase are given a portion of the money in escrow. In some applications additional proofs of knowledge are used in this phase.

To state the protocol more formally, we define the parties in SPIES (see Figure 1) as: Alice, the service provider; Bob, a consumer paying for access to the server; an escrow service E; and a set of charities Z with no active participation in the protocol. We denote the password as ϕ, and the end of the subscription period as time τ. The amount of money that Bob and Alice place in escrow with E is $\$(v)$. Finally, we denote any unauthorized possessors of the content (who may have obtained the content through theft or through unauthorized sharing) by $U_1 \ldots U_l$.

It is helpful to have a semantic description and a serial number for ϕ; in our protocol we will write this $d(\phi)$ (e.g., "password for service to slate.com"). We denote the exchange of x dollars as $\$(x)$. The transfer of such funds can be done by any secure method; e.g., credit cards over SSL.[1]

3.1 Protocol Details

Phase 1: Exchange. Alice registers a description of the secret $d(\phi)$ and the ending time τ with the escrow agent E. Bob and Alice place $\$(v)$ at risk. Alice then sends Bob a copy of ϕ. This should be done in a fair manner, such as with a protocol for fair exchange [1], so that Alice shares ϕ only when Bob has placed $\$(v)$ at risk, but we do not require a specific mechanism. At the end of this step, $\$(2v)$ is legally at risk if ϕ is revealed, and both Alice and Bob have knowledge of the secret ϕ.

Written in our notation, phase 1 is as follows:

$$Alice \rightarrow E \quad : \quad d(\phi), \tau \tag{1}$$

$$Alice \rightarrow E \quad : \quad d(\phi), \$(v) \tag{2}$$

$$Bob \rightarrow E \quad : \quad d(\phi), \$(v) \tag{3}$$

$$Alice \rightarrow Bob \quad : \quad \phi \tag{4}$$

Phase 2: Registration. Using some out-of-band means,

[1]For the sake of clarity, our details omit the fact that, where necessary, each party's message is signed for authenticity and integrity using previously setup up public or shared keys.

Variable	*Description*
ϕ	The protected secret
$d(\phi)$	The textual description of ϕ
$H(\phi)$	The hash of ϕ
τ	End time of secret protection
A	Provider of the secret (Alice)
B	Consumer of the secret (Bob)
E	A trusted escrow service
C	A set of charities
$z \in Z$	one randomly-chosen charity
$U_1 \ldots U_l$	Unauthorized possessors of ϕ
ρ	The total number of registrants
$\$(v)$	Alice or Bob's at-risk money
$\$(2v)$	The total amount of money at risk
$f(\rho)$	The share size function, dependent on the number of registrants

Figure 1: Variables used in SPIES

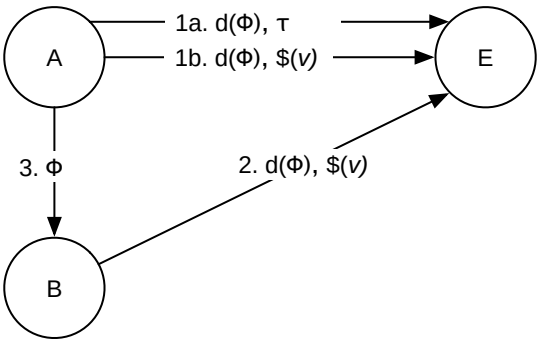

Figure 2: Phase 1: content is registered, monies are escrowed, and content is transfered.

E publishes widely that it is seeking anonymous registrations from anyone holding content described by $d(\phi)$. This includes all users, $U_1 \ldots U_l$, that have obtained the contained without participating in the above protocol — whether shared or stolen from either Alice or Bob. As we will show, because of the incentives, we expect to receive a single registration from each party: Alice, Bob, and from each U_l, if any. The protocol remains effective if not all legitimate possessors register or if some possessors (legitimate or not) register more than once.

First, Alice sends a hash of the content to E, denoted as $H(\phi)$ below; being able to generate this hash is what will serve as proof of possession of ϕ without revealing the secret to the escrow service. The main registration phase then begins, in which each registrant sends in the content description and a hash of the content. (Although Alice does not send in the hash again, she is considered one of the registrants.) Denote the total number of registrations by $\rho = l + 2$; if no unauthorized sharing has occurred then we expect $l = 0$ and $\rho = 2$.

If the content is more complex than a password string, the hash serves as a commitment to the content. In the case of a dispute, i.e. when a registrant has received a slightly modified copy of the content, the registrant must submit her full copy to show that she has the content. The escrow service can judge whether the copy matches the original during

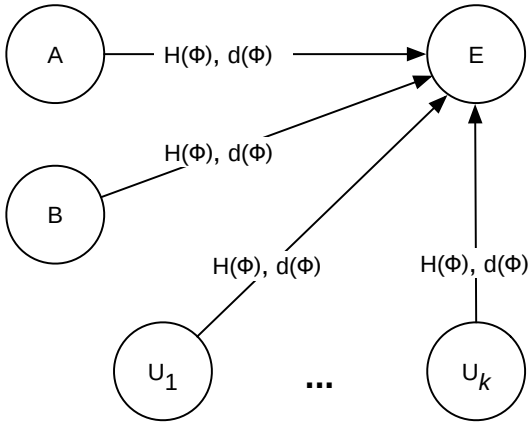

Figure 3: Phase 2: anonymous registration by possessors of the content.

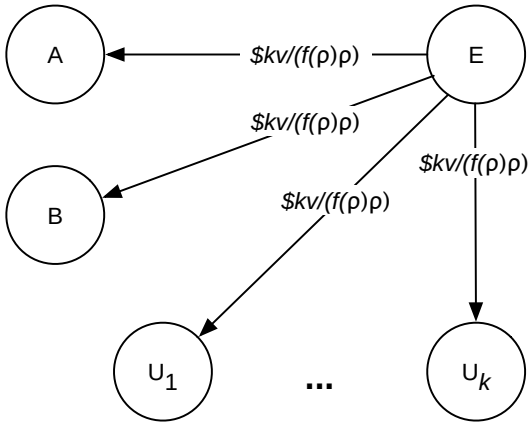

Figure 4: Phase 3: escrowed monies are distributed as $\$(2v/(f(\rho)\rho))$ per person.

phase three.

$$Alice \rightarrow E \quad : \quad H(\phi), d(\phi) \tag{5}$$
$$Bob \rightarrow E \quad : \quad H(\phi), d(\phi) \tag{6}$$
$$U_1 \rightarrow E \quad : \quad H(\phi), d(\phi) \tag{7}$$
$$\vdots$$
$$U_l \rightarrow E \quad : \quad H(\phi), d(\phi)$$

Phase 3: Payment. The last step, beginning at time τ, is the payment process. Each registrant will get some money: at most $1/\rho$ of the total amount in escrow[2]. If more than two registrations appear during the registration phase, registrants will each get strictly *less* than $1/\rho$ of the total

[2]If money was not placed in escrow but rather legally at risk (for example, a credit card authorization), Alice and Bob will receive the elimination of some or all of their legal liability instead: any money going to any other party will have to be paid for by them, just as if they had placed money in escrow.

amount: they will get $1/(f(\rho)\rho)$, with $f(\cdot)$ to be described later.

$$E \rightarrow Alice \quad : \quad \$\left(\frac{2v}{f(\rho)\rho}\right) \tag{8}$$

$$E \rightarrow Bob \quad : \quad \$\left(\frac{2v}{f(\rho)\rho}\right) \tag{9}$$

$$E \rightarrow U_1 \quad : \quad \$\left(\frac{2v}{f(\rho)\rho}\right) \tag{10}$$

$$\vdots$$

$$E \rightarrow U_l \quad : \quad \$\left(\frac{2v}{f(\rho)\rho}\right)$$

Function $f(\cdot)$ exists to deal with the problem of multiple dummy registrations by a single participant. Clearly, no participant should be allowed to get more than her fair share by sending in a huge number of registrations. Here, we state the requirements for $f(\cdot)$ so that, regardless of how many registrations have occurred, the payout to a cheater does not increase when she adds one more registration. In other words, the optimal strategy for all economically independent participants should be to register exactly once with E. We have three restrictions:

1. For $\rho < 2$, we need $f(0) = 2/\rho$ and $f(1) = 2/\rho$ to cover the exceptional case that either Alice or Bob fails to submit their registrations in time, though this should never occur with rational parties. In this special case each registrant receives exactly $\$(v)$.

2. For $\rho = 2$, we need $f(2) = 1$, so that when there are no unauthorized users, the payouts are not modified.

3. For $\rho > 2$ we need $f(\cdot)$ to be a function that grows sufficiently quickly that it is not possible for any participant to get more than her fair share (i.e., $2v/\rho$) by submitting multiple registrations.

We define such a function in Section 3.2.

Because of the effects of $f(\cdot)$, whenever more than two registrations with E occur, the total amount of money E gives out to registrants will be strictly less than the amount E holds in escrow. The remaining money is given to a randomly chosen charity $z \in Z$; the set Z is agreed upon between Alice and Bob before escrow and content exchange occurs. No charity in Z has any involvement in the protocol other than to serve as a destination for money that is not given to protocol participants.

$$E \rightarrow c \quad : \quad \$\left(2v(1 - \frac{1}{f(\rho)})\right) \tag{11}$$

If desired, a secure random coin flip protocol (e.g., see Schneier [10] p.89 for examples) can be used among the originally authorized content holders to choose a charity. Otherwise the trusted escrow service simply randomly decides on a charity.

The reason we chose a large set of charities is it increases the difficulty for a content holder to collude with a charity. For example, if there were only a single charity in Z, then Alice could make a deal to split the escrowed money between the two of them. Or, Bob could purposely release the content as an indirect method of increasing the funds available to his favorite charity. Increasing the set Z to a large number of charities (with disparate agendas) decreases the chances that an arbitrary authorized content holder can make agreements with the single charity z that is chosen in the end. The set Z can be made arbitrarily large to decrease the probability of successful collusion.

Note that since $f(2) = 1$, the charity gets no money in the case that no unauthorized sharing occurred.

This completes the description of the protocol; the payout function $f(\cdot)$ is described in greater detail below.

3.2 Designing the Payout Function

The main requirement for $f(\cdot)$ is that it create a disincentive for registering more than once. We require that a party adding an additional dummy registration, and thus getting an additional share of the money in escrow, get strictly less total money. In the worst case, Alice may behave honestly and submit one registration while Bob submits k registrations, so that Bob registrant receives $k/(k+1)$ of the shares. The size of the shares for the $k+1$ case must be decreased sufficiently that the k shares together are strictly less than one of the larger shares.

Suppose that, before Bob has registered, there are α existing registrations, and $\$(p)$ in escrow; Bob can choose any number β of registrations to add, to obtain β shares each of size

$$\$\left(\frac{p}{(\alpha+\beta)f(\alpha+\beta)}\right)$$

We need a function $f(\cdot)$ that will make the total returned to Bob

$$\$\left(\frac{\beta p}{(\alpha+\beta)f(\alpha+\beta)}\right)$$

maximum at $\beta = 1$ and strictly decreasing as β increases.

The exponential function

$$f(x) = 2^{x-2}$$

satisfies the requirement. Bob will have a total return of

$$\$\left(\frac{\beta p}{(\alpha+\beta)2^{\alpha+\beta-2}}\right)$$

which is maximum at $\beta = 1$. When $\alpha + \beta = 2$, which happens when there is only one registration each from both Alice and Bob, $f(\alpha+\beta) = 2^0 = 1$ and all the money in escrow is returned to the contributers. Since the maximum with respect to β does not depend on the number of prior registrations α, it is still in Bob's interest to register exactly once even when there are more than k registrations.

3.3 Examples of SPIES Applications

Our primary example of the use of SPIES is protection against reselling of access to a service: Alice owns a company that provides wireless network access at coffee shop hotspots around the country. She offers Bob a fee-based monthly subscription to the service.

Alice could simply accept payment from Bob then provide him with a username/password pair that he can use at any hotspot. However, Alice would then risk Bob sharing his password with multiple friends. Even worse, Bob, or any one of these friends, may post the username and password on the Internet, providing cost-free access to an unbounded set of strangers. By using SPIES to protect the password (the content ϕ), Alice can reduce this risk. Further, in this

scenario, Alice need not put money in escrow and can even act as the escrow service; she has a clear disincentive to give Bob's password away.

Forcing Bob to put money in escrow is a disincentive for him to purchase the service. However, in this example, Bob can authorize payment on his credit card in the case the unauthorized users register the password with the escrow. This model is similar to the one used in some rental agreements: in lieu of a deposit, the rental company keeps a payment authorization in case the rental is damaged or not returned.

SPIES does not prevent Bob from reselling the service to others; however, as we show in Section 3.4, by setting the escrow amount correctly, we can discourage Bob from reselling.

One implication of SPIES is that it shifts some of the burden on protecting passwords to the consumer; a hacked computer can mean lost money. However, the provider could give the consumer one day or more to report a stolen password, where all registrations during that one day are ignored. A new password can be generated at that point. This still provides the user with an incentive to change her password quickly after such a break-in. Consumers who repeatedly lose passwords can have their subscriptions revoked.

There is a broad range of uses for SPIES, as the following examples illustrate.

Non-disclosure Agreements. Alice owns large software company that is developing a new product and would like to outsource some of the project to Bob. Alice is worried that Bob might disclose the software on the Internet or with her competitors. Therefore, Bob places money in escrow for the duration of the project. If Bob shares the content with anyone, or anyone breaks his security and obtains a copy of the content, he will lose the money in escrow. If Bob does not trust Alice (or the quality of her security infrastructure), he may ask her to place money in escrow as well. The money Bob places in escrow is not the opportunity cost of Alice's loss, but rather the smaller amount necessary to provide incentive for Bob to protect the content.

Entertainment Reviews. Alice produced a movie or video game and would like Bob's magazine to review the content. Alice and Bob place money in escrow and until just before the product will be available to the general public. The money placed in escrow is not equal to the opportunity cost Alice will lose from people downloading the content from the Internet. It is equal to the amount that Bob would expect to profit from by selling the content. Keep in mind that Bob is not going to make millions of dollars from a preview of a movie as he does not have the distribution network that Alice has. Realistically, Bob could sell to a few people on the Internet, who may then offer the content themselves, either as resellers or freely on a p2p network. The value of Bob's content once he releases it is very low, and it is this that is his security payment, not Alice's much larger potential loss.

Exclusive Access to a Photograph. Alice is a freelance photographer and has an exclusive shot (or movie) of an important news event. She sells rights to publish the photo to Bob's newspaper. However, Bob does not trust that Alice will not sell the photo to anyone else first. Bob places the purchase price, $\$(w)$ in escrow plus an additional amount, $\$(x)$. If no one else registers with the escrow service, then Alice receives the purchase price, and Bob receives back his additional amount. If there are three or more registrations, then the amount deducted from escrow and given to charity follows the payout formula given in Section 3.2.

3.4 Setting the Security Deposit Amount

Bob may share his password to a subscription service for political or personal reasons, or he may sell it for financial gain. The security deposit must be set high enough to be a deterrent to both. It is likely that if it is high enough to prevent any profiting from sales, it will also be high enough to deter sharing for non-financial reasons. At the same time, the security deposit should be set as low as possible, since it acts as a disincentive for Bob to participate in the protocol at all.

Suppose that the subscription service is priced at $\$(c)$ per protection period. Bob probably can not sell his password for more than $\$(c)$, since at that price, the honest buyer could simply obtain the service legitimately from Alice.

We can set $\$(cx)$ as an upper bound on the profit Bob can make on selling the secret to x buyers; in practice it will be less, since the buyers themselves can share, or sell, the received password to others in competition with Bob, and since there may be a limited market. In the most general case, Alice would have to estimate how much money Bob could make, and set the security deposit to that amount: $v = cx$.

However, for many subscription services there is some number of users at which it becomes trivially obvious to Alice that more than one user is accessing the account; for instance, if a user logs in simultaneously more than some number of times. Call this number n: Alice will deactivate the account if more than n users have access. Buyers know that the password will be useless if sold to more than n persons, so Alice can set the security deposit to $v = c(n + 1)$ and Bob should be unable to sell his password that many times to rational buyers. (See Section 4.3.2 for a discussion of this escrow setting.)

If $n = 2$ then clearly SPIES is unnecessary; we expect that n is larger than two in almost all cases, but varies for different services. For example, subscribers to consumerreports.com do not often check the site everyday; therefore it would easy to share passwords among a large group without concurrent usage. Subscribers to salon.com may use the site everyday, and detecting concurrent usage of a smaller number of users may be easier for the provider.

3.4.1 Setting Escrow for Content

When SPIES is used to protect content itself, the security deposit should be enough to exceed Bob's potential gain from selling the content, *not to cover Alice's lost revenue.* For instance, although Bob sharing a pre-release of a movie on the Internet might cause millions of dollars of losses to the movie studio, Bob cannot possibly make as much money by selling the movie without the studio's distribution network and without being found out and sued by the studio. Furthermore, once Bob has shared the content with even one buyer, he must contend with that buyer potentially setting herself up as a competitor and selling or sharing the con-

tent. A reviewer might not be able to put millions of dollars at risk to get access to a movie, but could potentially place at risk the amount of money he could realistically stand to gain by selling it himself.

The security deposit also serves as incentive to increase security and prevent access to the secret. For example, a reviewer of a well-known magazine may be trusted to not sell a review copy of a movie on the black market; the escrowed money acts as incentive for preventing her teenage son from gaining access to the content, because she knows it would cost her several thousand dollars for the movie to end up a peer-to-peer file sharing network. Content producers already have trust mechanisms in place for releasing content in this fashion and we believe SPIES is a mechanism that adds robustness to those relationships.

One important caveat here is that Bob must believe that Alice will protect the content and not otherwise give it away. This is reasonable, since Alice must has the duel incentive of not losing potential sales and of not losing her escrowed deposit. If Bob believes that Alice might fail to protect the content, he has an added incentive to sell the content, as his security deposit might not be there in any case.

In all cases, SPIES does not provide recompense to the content owner if content is released before time τ. SPIES could be altered to provided such recompense, but that would give an incentive for the owner herself to release the content.

4. STRATEGIES OF THE PARTICIPANTS

In this section, we characterize the SPIES protocol and the participants' choices in game-theoretic terms [8]. We model an execution of the protocol as a strategic game. The game is not repeated and the participants chose their actions independently. First, we describe a model of the *utility* of actions in the protocol and then we show how various actions lead to different utility values for each type of actor in the game.

4.1 Actions

The utility of an action has two components: *monetary* and *intrinsic*. We consider the effect of actions on each component in turn.

Monetary Utility. We assume participants receive some utility from money and will try to maximize the money they have. We distinguish the money available through the escrow service and through sale of the secret or content.

There are two types of actions the participants can take in our protocol: *registering* with the escrow service and *sharing* the secret, ϕ, with third parties. We do not distinguish between intentional and unintentional sharing; we consider lax security equivalent to intentional sharing. Participants can choose to pay into the escrow service (or to authorize a payment if later needed) or not; we treat this payment as equivalent to choosing whether to participate in the protocol.

If a participant can sell the content widely, then the sales may overwhelm any other incentives in the protocol — we discuss this possibility in more detail in Section 3.4.

Intrinsic Utility. The content may have some intrinsic utility. For instance, a password could allow access to a useful service; a training video could teach a useful skill to someone watches it. A more interesting case of intrinsic utility is when an operating system developer could share unreleased, future designs and programming libraries with a designer of third-party applications. In this case, each party gains intrinsic utility: the operating system developer ensures that new applications will use the capabilities of the new operating system, while the applications developer gets to produce the first set of software for the new operating system. Although we measure intrinsic utility with monetary values, we specifically regard intrinsic utility as *not* including the monetary utility of selling the content.

4.2 Outcomes

An outcome in SPIES is described by the variables

- Q: The set of authorized possessors with access to ϕ; this is fixed through the protocol. In this paper we consider the set consisting of A, the secret provider, and B, the content user, so $|Q| = 2$.
- U: The set of unauthorized possessors with access to ϕ.

4.3 Utility Functions

We define:

- $\mathbf{intrinsic}_p$, the intrinsic value of ϕ to participant p;
- $\mathbf{share}_A^B$, the value for A of sharing the content with B, either as a direct monetary payment or the intrinsic value of collaboration;
- $\mathbf{harm}_p^q$, the monetary harm (for example, loss of sales) to participant p when a copy of ϕ is obtained by participant q;
- Δ_p, which indicates whether participant p paid into the escrow service, and is 0 for $p \in U$, 1 for B and A, the members of Q;
- $\mathbf{cost}_p$, participant p's cost to get access to ϕ; for example, a payment to an individual who has it.

4.3.1 Data Owner

Let $\bar{C}$ be A's expected harm from sharing if she does not use SPIES:

$$\bar{C} = E\left(\sum_{q \in U} \mathbf{harm}_A^q | \overline{\text{SPIES}}\right).$$

Let C be A's expected harm from sharing if she does use SPIES:

$$C = E\left(\sum_{q \in U} \mathbf{harm}_A^q | \text{SPIES}\right).$$

A can choose to not share the content; to share the content without using SPIES; or to share the content using SPIES. Her utility μ_A varies accordingly.

$$\mu_A = \mathbf{intrinsic}_A \tag{12}$$

if she does not share;

$$\mu_A = \mathbf{intrinsic}_A + \mathbf{share}_A^B - \bar{C} \tag{13}$$

if she shares without using SPIES; and

Participant	*Strategy*	*Utility*
A	don't share	$\mathbf{intrinsic}_A$
	share	$\mathbf{intrinsic}_A + \mathbf{share}_A^B - \bar{C}$
	use SPIES	$\mathbf{intrinsic}_A + \mathbf{share}_A^B - C - v + \frac{2v}{f(\rho)\rho}$
B	do nothing	0
	participate honestly	$\mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(R)R}$
	sell content	$\mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(R')R'} + \mathbf{sales}_B$
U_i	–	$\frac{2v}{f(\rho)\rho} + \mathbf{intrinsic}_{U_i}$

Figure 5: Participants' Utilities

$$\mu_A = \mathbf{intrinsic}_A + \mathbf{share}_A^B - C - v + \frac{2v}{f(\rho)\rho} \quad (14)$$

if she uses SPIES.

If she is rational, she will use SPIES if the third case has higher utility than the other two. SPIES is superior to not sharing at all when

$$\begin{aligned} \mathbf{intrinsic}_A + \mathbf{share}_A^B - C - v + \frac{2v}{f(\rho)\rho} &> \mathbf{intrinsic}_A \\ \mathbf{share}_A^B - v + \frac{2v}{f(\rho)\rho} &> C \end{aligned} \quad (15)$$

Sharing with SPIES is superior to sharing without SPIES when

$$\begin{aligned} \mathbf{intrinsic}_A + \mathbf{share}_A^B - C - v + \frac{2v}{f(\rho)\rho} &> \\ &\mathbf{intrinsic}_A + \mathbf{share}_A^B - \bar{C} \\ \bar{C} - v + \frac{2v}{f(\rho)\rho} &> C \end{aligned} \quad (16)$$

If A does use SPIES, it is clear that by submitting more than one registration she is raising ρ and will reduce the portion of v returned. Therefore, it is in her interest to submit only one registration.

We can quantify A's utility in Equations 15 and 16 if we consider our primary example: sales of a subscription service, when the password is the content. A's intrinsic value is

$$\mathbf{intrinsic}_A = 0;$$

the password is useless to her. Let the price of the service over the protection period be

$$\mathbf{share}_A^B = c,$$

and let us assume that the incremental cost of providing service to B is negligible (it is easy to show that adding this cost does not affect the analysis). As described in Section 3.4 for this example, assume that A has set the escrow amount as

$$v = c(n+1),$$

which is c times one more than the minimum number of unauthorized users n required to make detection of unauthorized use trivial for A.

A should use SPIES if she believes that she will have greater utility than not offering the service at all, and greater utility than offering the service without using SPIES. The first is true when

$$c - c(n+1) + \frac{2c(n+1)}{f(\rho)\rho} > C. \quad (17)$$

As we will show below, because of the way A has set the escrow amount, she expects B *not* to share the password at all. So she expects $\rho = 2$, $C = 0$. Thus, A will choose SPIES over not sharing the password at all when $c - c(n+1) + c(n+1) > 0$, which reduces to $c > 0$.

On the other hand, SPIES is superior to sharing the password without using SPIES when

$$\bar{C} - c(n+1) + \frac{2c(n+1)}{f(\rho)\rho} > C. \quad (18)$$

Again A expects $\rho = 2$, $C = 0$, so her best strategy is to use SPIES when $\bar{C} > 0$; in other words, when she expects that the user might share the password when SPIES is not used.

4.3.2 The Authorized Possessor

For B, $\mathbf{harm}_B = 0$, as we assume that he does not lose value directly from the sharing of the content.

His options are to not participate in the protocol, to participate and behave honestly, and to participate and sell the content. Again, his utility varies for each. It is:

$$\mu_B = 0 \quad (19)$$

if he does not participate;

$$\mu_B = \mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(\rho)\rho} \quad (20)$$

if he participates honestly, and

$$\mu_B = \mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(\rho)\rho} + \mathbf{sales}_B \quad (21)$$

if he participates and then sells the content. $\mathbf{sales}_B$ is the income B expects to make from sales of ϕ.

B will expect ρ to depend on whether he sells the content. Let his expected value of ρ if he does not sell the content be R, while his expected value if he does sell is R'.

If rational, B will participate honestly if it is superior to the other two options. Honesty is a better strategy than not participating when

$$\mathbf{intrinsic}_B > \mathbf{cost}_B + v - \frac{2v}{f(\rho)\rho}. \quad (22)$$

Honesty is superior to participating and selling the content, which occurs when the increase in ρ caused by selling

the content offsets any profit made from sales,

$$\frac{2v}{f(R)R} > \frac{2v}{f(R')R'} + \mathbf{sales}_B. \quad (23)$$

Again we see that if he does use SPIES his best strategy is to register exactly once whether he sells the secret or not.

Consider again the service password example. We will now show that for B's best strategy to be to sell the content, he must sell so many copies of the password that the abuse will be detected by A.

Let $\mathbf{cost}_B = c$ and $v = c(n+1)$. B expects $\rho = 2$ if he does not sell, so $R = 2$.

B is not likely to be able to sell at a price higher than c, since A offers the service at this price. If he sells to x persons at a price of c, he expects $\mathbf{sales}_B = cx$. He expects ρ to be at least $x+2$; as we will show, all the persons he sold to have an incentive to register, as well as A and B. So $R' = x+2$. Recall that the the escrow amount is set at $c(n+1)$, where n is the number of users that lets A trivially detect improper use of the account.

It is in B's interest to participate honestly rather than to not participate at all when his benefit from the service exceeds his cost; in other words when

$$\begin{aligned} \mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(\rho)\rho} &> 0 \\ \mathbf{intrinsic}_B &> c + c(n+1) - c(n+1) \\ \mathbf{intrinsic}_B &> c \end{aligned} \quad (24)$$

It is in his interest to sell the content rather than participate honestly when

$$\begin{aligned} \mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(\rho)\rho} &< \\ \mathbf{intrinsic}_B - \mathbf{cost}_B - v + \frac{2v}{f(\rho)\rho} + \mathbf{sales}_B & \\ \frac{2v}{f(R)R} &< \frac{2v}{f(R')R'} + \mathbf{sales}_B \end{aligned}$$

Letting $v = c(n+1)$, $R = n$ and $R' = x$, we have:

$$\begin{aligned} c(n+1) &< \frac{2c(n+1)}{(x+2)2^x} + cx \\ n+1 &< \frac{2(n+1)}{(x+2)2^x} + x \\ n+1 - \frac{2(n+1)}{(x+2)2^x} &< x \end{aligned} \quad (25)$$

As x increases, $\frac{2(n+1)}{(x+2)2^x}$ quickly becomes less than one. So B must sell his password at least $n+1$ times just to cover the loss of the escrow amount $c(n+1)$. However, the password becomes useless if there are n or more users. Potential buyers, knowing that B must over-sell the password to break even, should be unwilling to buy. If B sells at a price less than c, he must sell even more to break even. If the intrinsic value of the service is sufficient to B that he wants to pay for it, he should conclude that the most sensible action is to participate and not sell the content.

4.3.3 Unauthorized Possessors

For an unauthorized possessor, U_i, $\mathbf{harm}_{U_i} = 0$ and $\Delta_{U_i} = 0$. U_i's expected utility is

$$\mu_{U_i} = \frac{2v}{f(\rho)\rho} + \mathbf{intrinsic}_{U_i}. \quad (26)$$

U_i is not a participant; her only choices are the number of times to register and whether to further share the content ϕ. The term $\frac{2v}{f(\rho)\rho}$ is maximized when she registers exactly once and does not share ϕ.

It is in the interest of U_i to sell if she can make more by selling than she will lose in her payment by increasing ρ. When ρ is large, her payment from the escrow service will be very small so it will be in her interest to sell. It is difficult to know what price a buyer might be willing to pay at this point.

In the example of the password protected service, a buyer should consider that it is in B's interest to try to sell the password at least $n+1$ times. If she believes that B is rational, she should expect that the password is useless and not be willing to buy it.

4.3.4 Escrow Service

We assume that E honestly performs the job of an escrow service. E cannot honestly get a copy of ϕ before the end of the protection period, so her sole decision is whether fake her own registration. It is clearly in her interest to do so exactly once. Therefore, we assume that not doing so is part of honest escrow operation.

4.3.5 Charity

No charity in the set C has access to ϕ. It is in the interest of all charities in C to register, but they cannot do so without ϕ. If some charity can gain access to ϕ, for instance by collaboration with another participant, she can obtain essentially all of $2v$ by making a large number of anonymous registrations.

What deters charities and authorized participants from colluding is the random selection of the exact charity until the end of the registration period. There is a direct relationship between the size of the set C and the difficulty of collusion.

If the size of C is large, this increases the number of entities with an incentive for having the content released into the public domain. However, if the number of charities is large, each individual charity's expected utility would be small since there would only be a small chance they would be chosen randomly.

Finally, we note that the large set of charities could join forces to gain access to the content. Joining forces does not increase their expected utility — i.e., there is a cost in doing this, and the utility would be divided among them. If this incentive is a concern, the protocol can be modified to not send any money to charities; all money that would go to a charity is instead converted to hard currency and destroyed.

4.4 Summary of Strategies

The content owner has an incentive to participate in the protocol when there is some benefit from sharing the content and harm from sharing the content widely. The other participant has an incentive to participate when the content is sufficiently valuable that they are willing to risk some or all of their escrow payment v. Unauthorized participants have an incentive to register exactly once and reduce their share of escrowed money for each person they share with. The escrow service can at worst take a portion of the money in escrow but cannot share the content. The charity can take essentially all of the money in escrow if she can get the

content or otherwise spoof registration; this is a limitation of the protocol.

SPIES does not provide an incentive for a participant not to share content with those that are not economically independent from the participant or who are fully trusted not to take advantage of knowledge of the content by submitting registrations to the escrow server. Although this is a limitation, we believe that in many cases this is a reasonable degree of content sharing to allow, and such sharing is inherently very limited.

5. CONCLUSIONS

SPIES is the first work, to our knowledge, that provides a negative incentive for distribution of digital content beyond authorized possessors. There are three simple steps: exchange of the secret and placement of funds in escrow; registration of content holders; and release of escrowed funds to registrants. The protocol can be repeated periodically for password protected services.

We have analyzed the best strategies of all participants. For the secret provider, the best strategy is to use SPIES when the secret has value and expects the consumer has incentive to re-sell the content. The consumer of the content gains the most utility from purchasing the content, placing money in escrow, and not re-selling or distributing the content, so that the escrowed funds are returned.

SPIES is simple to implement and is applicable to many scenarios. We have provided examples for password-secured web sites, password-secured services, non-disclosure agreements, entertainment reviews, and exclusive access to media.

6. REFERENCES

[1] Bao, F., Deng, R., and Mao, W. Efficient and Practical Fair Exchange Protocols with Off-Line TTP. In *Proc. 1998 IEEE Symposium on Security and Privacy* (May 1998).

[2] Berthold, O., Federrath, H., and Kohntopp, M. Project Anonymity and Unobservability in the Internet. In *Computers Freedom and Privacy Conference 2000 (CFP 2000) Workshop on Freedom and Privacy by Design* (April 2000).

[3] Golle, P., Leyton-Brown, K., Mironov, I., and Lillibridge, M. Incentives for Sharing in Peer-to-Peer Networks. *Lecture Notes in Computer Science 2232* (2001).

[4] Horne, B., Pinkas, B., and Sander, T. Escrow Services and Incentives in Peer-to-Peer Networks. In *Proceedings of the 3rd ACM Conference on Electronic Commerce* (2001).

[5] Levine, B. N., and Shields, C. Hordes — A Multicast Based Protocol for Anonymity. *Journal of Computer Security 10*, 3 (2002), 213—240.

[6] Margolin, N. B., Wright, M. K., and Levine, B. N. SPIES: Secret Protection Incentive-based Escrow System. In *Proc. Workshop on the Economics of Peer-to-Peer Systems (p2pecon)* (June 2004).

[7] Microsoft DRM Technologies Establish Foundation For Emerging Internet Music, Video and eBooks Industries. Microsoft Press Release, June 2001.

[8] Osborne, M. J., and Rubinstein, A. *A Course In Game Theory*. MIT Press, 1994.

[9] Reed, M., Syverson, P., and Goldschlag, D. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection* (1998).

[10] Schneier, B. *Applied Cryptography*. John Wiley & Sons, 1996.