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
ACM Digital Rights Management 2004
Protecting Passwords

- Passwords grant access to e.g. a paid subscription service
- Passwords can be easily copied, posted online, shared with friends...
- Service provider loses money / potential customers
Approaches to Protect Access to Accounts

- **Enforcement:** turn off account, sue subscriber
  - detect inappropriate use: too many simultaneous logins, disparate IP addresses
    - problem of false positives

- **Prevention:**
  - only one login at a time
    - but you can still have sharing...
  - Tie login to one computer by hardware signatures, IP address, MAC address

- **Incentives**
Our approach: SPIES
(Secret Protection Incentive Based Escrow System)

- Provide financial incentive not to share
- Applicable to content that
  - is not widely available
  - needs to be protected a short while
- Best application: protecting passwords
Features of SPIES

• no hardware or software restrictions
  – compatible with any type of device
  – password can be backed up
  – password can be stored on different devices

• password can be shared with anyone trusted
  – friend keeps a copy for emergencies, like house–keys
  – can have third–party backups
Players in SPIES

- Alice, a password provider
- Bob, a customer
- A trusted escrow service
- A charity
Basic Operation of SPIES

- Bob gives a security deposit to an Escrow service.
- Anyone who has the password can present proof of possession to the Escrow service ("register") for a payment.
- At the end of a protection period, Bob’s security deposit is returned. It is reduced if someone presents such proof.
SPIES Protocol Phases

- Exchange
- Registration
- Payment

Protection Period
Phase 1: Exchange

- Alice gives the password to Bob
  - typically: Bob gives some payment to Alice too
- Alice and Bob give a security deposit to Escrow,
- Alice sends a hash of the password to Escrow
- Alice and Bob are the “legitimate possessors”
Phase 2: Registration

- Bob and Alice present proof of password possession to the Escrow Service
  - hash of the password
- So does anyone else who somehow has access to the password, whether stolen or bought
  - this registration can be anonymous
Phase 3: Payment

- Escrow pays ALL registrants, legitimate or not.
- Alice & Bob lose some of their deposits if there are illegitimate registrations.
- Charity gets excess money if sharing occurred.
Setting the Security Deposit

• It should not be so high that Bob won’t participate
• It should be more than Bob can get in total by selling the password
  – Can be difficult to determine
• One way to determine security deposit level: detect multiple people using an account
Account Limits for Setting the Security Deposit

- Suppose that use of an account by x or more people can be detected, and account disabled
- Set escrow amount so Bob would need to sell to more than x to recover escrow
- Unauthorized possessors shouldn’t buy
  - Bob is probably selling a worthless password
  - Other buyers may have resold as well
- Bob probably won’t be able to make a net profit. He shouldn’t sell at all.
Attacks on SPIES

- Alice registers twice to get Bob in trouble
  - she loses her escrow
- Alice shares the data with someone else
  - she loses her escrow
- Someone registers many times
  - exponential payout function: they get \textbf{less} money total
  - charity gets non-distributed money
Exponential Payout Function

• Each registrant gets only $\frac{1}{2^{x-2}}$ of the amount they would get where $x$ is the number of registrations.

• Example: $5$ deposit
  - Alice and Bob register once; each gets $\frac{1}{2^0}$ of $5$, i.e. $5$
  - Bob makes 5
    • there are 6 shares (Alice’s 1 plus 6 for Bob)
    • Each share gets $\frac{1}{2^{(6-2)}} = \frac{1}{16}$ th of $5$
    • Bob gets $\frac{5}{16}$ of $5$ or about $\$1.56$, not $\$5$.
    • Alice only gets $\$0.31$!

• Details in paper
Strategies of Content Possessors

• Authorized Possessors
  - Don’t share unless you think someone else has
    • sharing reduces the returned security deposit
    • Different from Prisoner’s Dilemma!
  - register exactly once

• Unauthorized Possessors
  - If you have the content, register exactly once
  - don’t spread the content further – maybe.
    • depends on benefit, escrow amount, number of unauthorized possessors
Strategies of other participants

• Escrow: assumed to be honest
  – It can collaborate with a charity to get security deposits

• Charity: can get all the money if it gets the content
  – Use a large number of charities; secure coin flip to choose one
Nash Equilibria and Rationalization

- Def: given other’s actions, no one can improve their utility with different action
- We found two Nash equilibria: neither shares and both share.
  - Both do best if they don’t sell
  - If one sells the other does better to sell too
  - Still works with more than two participants
- Depends on being able to make a fixed, limited amount of money by selling
- If Bob knows Alice is rational & vice-versa, no-one shares: “rationalized” outcome
Key: Incentives Levels

• Can always ensure non-sharing
  – death penalty for authorized possessors if there are too many registrations

• To get users to participate, their expected utility must be positive

• Again, Alice prefers a high security deposit, Bob a low one; these must be balanced.
Other uses

- Non-disclosure agreements between companies
- Entertainment content shared to a reviewer pre-release
- Exclusive photographs shared with a newspaper by the photographer
- In these cases, the hash serves as a commitment: a human must determine if the content is identical – content can be obscured in many ways
Conclusion

• SPIES Provides an incentive to users
  – not to share
  – to protect their content

• useable as an additional layer of protection with other technologies and policies
  – DRM, Watermarking, lawsuits

• Applicable to passwords and other content