TheGRID™

Stop Subscription Sharing

With Device Authentication

e Lock

e-Lock Corporation Sdn Bhd

December 2009

Table Of Content

Executive Summary

The Issue
A paid online subscription web portal faces the issue of subscription account sharing whereby a single subscriber account is shared among multiple users with the intention to save subscription costs.

The Impact
The practice of subscription account sharing has a negative impact on the growth in subscriber base and potential revenue because multiple users are now sharing one paid subscription.

The Challenges
The challenges for mitigating this issue include:

- To assess the extent of account sharing and estimate potential revenue loss
- To implement an effective countermeasure to curb the abuse

A Common But Inadequate Countermeasure
A common countermeasure is to implement restriction on simultaneous login sessions per user account. However, time-sharing is still possible among users. A more effective solution is to adopt user device authentication to restrict each subscriber account to be accessible from a limited number of user-side devices.

The Solution
TheGRID is a user device identification and authentication solution commonly used for the following purposes:

- Two-factor authentication to double verify user identity during login to a web portal
- User device restriction to deter unauthorized account sharing

TheGRID solution offers the following benefits:

- Effective against unauthorized subscription account sharing
- Gathering of vital statistics on account sharing abuse
- Transparent user-end experience – no change in user login process
- Flexible device limit settings per user account
- Easy to implement and deploy

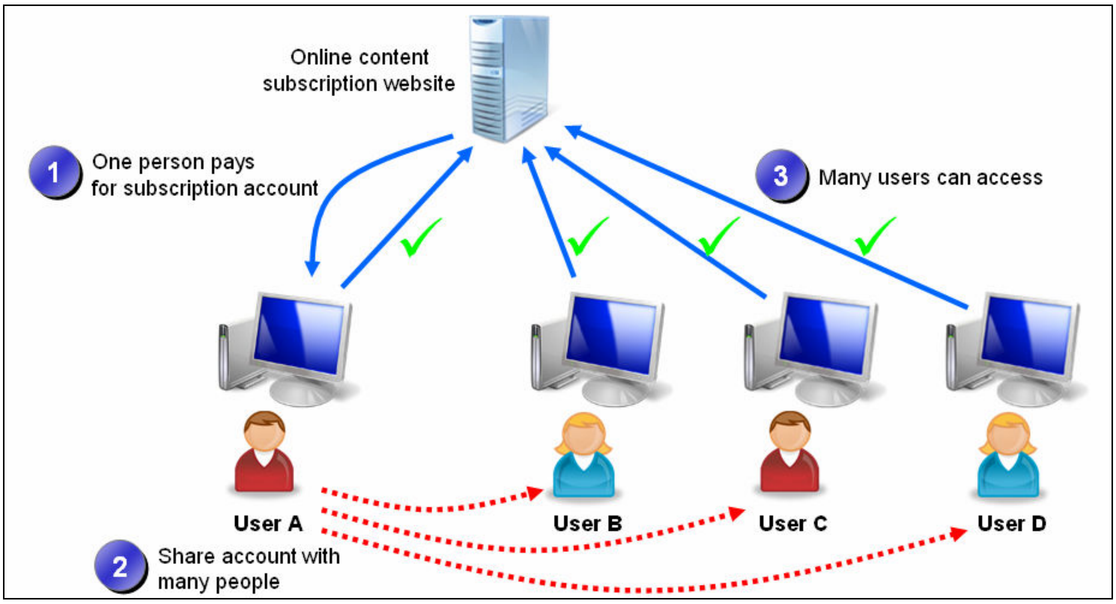
TheGRID has been deployed by online web portals from across the industry:

- Online paid content provider (e.g. PricewaterhouseCoopers eTax virtual library)
- Online banking (e.g. Alliance Bank)
- Online securities trading (e.g. SBI Securities, Japan)

1. Introduction

1.1 The Issue - Subscription Account Sharing

A paid online subscription web portal operates by providing online login accounts to its paying subscribers. However, quite commonly, the actual number of people accessing a particular paid subscription website is more than the number of its paying subscribers. This phenomenon is obviously due to the unauthorized sharing of a single subscriber account among multiple users with the intention of lowering the average subscription cost by sharing.


Online content subscription website
1 One person pays for subscription account
3 Many users can access
User A
User B
User C
User D
2 Share account with many people

1.2 The Impact – Loss of Potential Revenue

Since paid online subscription businesses rely on income from subscription payments, the practice of subscription account sharing might have a significant negative impact on the growth in subscriber base and potential revenue. A paid site could potentially generate higher revenue if it could deter the mal-practice of account sharing and encourage everyone who accesses the paid service to sign up as a paying subscriber.

1.3 The Challenges

1.3.1 How To Assess Abuse Severity and Estimate Potential Revenue Loss?

Firstly, it is difficult to assess the extent of the account sharing practice. There should be a reliable way to quantify the level of such abuse among the account holders. Vital statistics on the number of users sharing the same account would provide management insight into the severity of this issue, so that the loss of potential revenue can subsequently be estimated.

1.3.2 How To Implement Effective Countermeasures?

Implementing an effective countermeasure is easier said than done. One common countermeasure is to implement restriction on simultaneous login per user account. This is typically implemented at the web application layer to check and limit the total number of active login sessions per user account at anyone time. This countermeasure is effective to a certain extent by making unauthorized account sharing more inconvenient, which now prevents these users from sharing the account at any time they wish. However, account sharing is still possible with cooperative arrangements among these sharers by agreeing on the time to access the paid site for each person.

2. TheGRID – Stop Subscription Sharing

2.1 Overview

TheGRID is a user-end device identification and authentication solution commonly used for the following purposes:

- Two-factor authentication for additional validation for logins or transactions
- User device identification and restriction to deter unauthorized account sharing

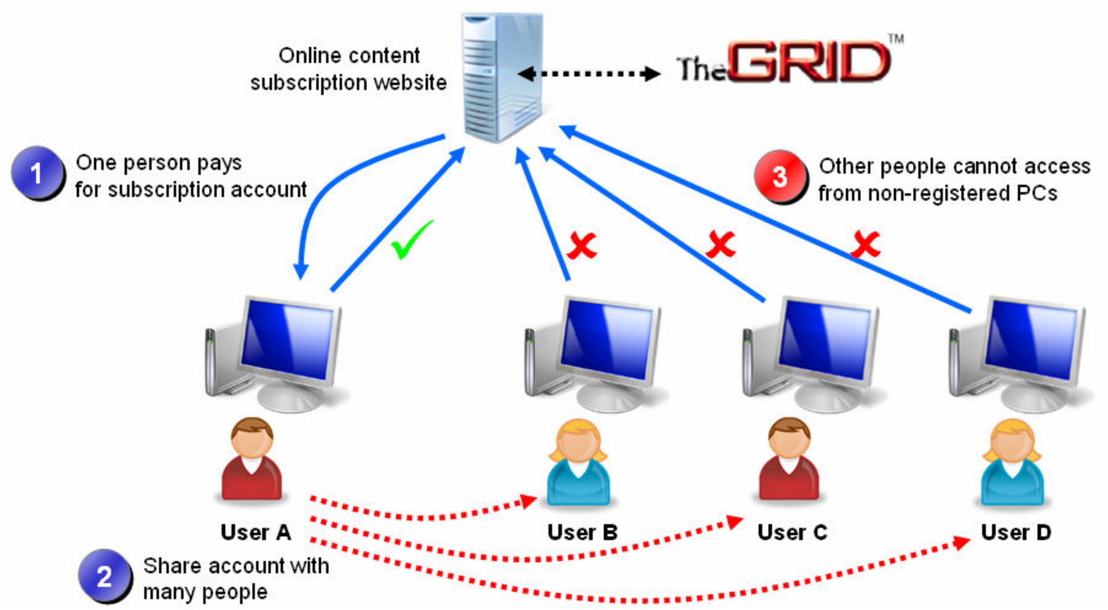
This paper focuses on objective to stop subscription sharing.

2.2 Gathering Vital Statistics on Unauthorized Account Sharing

TheGRID can be deployed in "monitoring mode" to gather information on how many different user-side devices are used to access each subscriber account. TheGRID is able to uniquely identify the user device on each incoming login connection and collect statistics on account sharing over a period of time. This "monitoring mode" implementation is totally silent and transparent to the users, and it is typically implemented to study the extent of subscription sharing abuse. With the information gathered, it is straightforward to estimate the total loss of potential revenue from the non-subscribing users.

2.3 Enforcing Device Limits To Curb Unauthorized Account Sharing

The real value of TheGRID comes when it is deployed to enforce account sharing restrictions by imposing a limit to the number of devices allowed for each subscriber account. Unauthorized account sharing now becomes extremely inconvenient because these users typically do not share their physical computers and they might not even be within a localized geographic location. The time-sharing of the subscription account is no longer possible.


Online content
subscription website
TheGRID™
1 One person pays for subscription account
3 Other people cannot access from non-registered PCs
✓
✗
✗
✗
User A
User B
User C
User D
2 Share account with many people

2.4 Key Benefits

2.4.1 Effective against unauthorized subscription account sharing

TheGRID is more effective in deterring unauthorized account sharing by limiting the device(s) that a user can use to log in to the paid site. Subscriber accounts are no longer subject to excessive abuse via time sharing or other unauthorized means.

2.4.2 Gathering of vital statistics on account sharing abuse

TheGRID is able to collect vital statistics on the extent of subscription account abuse by identifying the number of user devices used to access each subscriber account.

2.4.3 Transparent user-end experience – no change in user login process

TheGRID works transparently behind the scene without affecting user's experience at online web portal. There is no explicit change required on how the user accesses the website.

2.4.4 Flexible device limit settings per user account

TheGRID allows the paid site to set a default device limit for all the subscriber accounts, and yet at the same time allows flexible individualized device limit settings on a case by case basis. This allows easy management of policy change and individual exceptions.

2.4.5 Easy to implement and deploy

TheGRID can be easily integrated with many different types of web application platforms. At the same time, it is easy to deploy TheGRID to millions of users over the web without any explicit user-end efforts.

2.5 How It Works

1) Firstly, prior to the deployment, TheGRID system is integrated to the login access control module of the existing web application.
2) Each subscriber account is assigned a limit on the maximum number of devices (computers, notebooks, mobile, etc) that can be registered to access the paid site.
    a) The device limit is typically set to "1" for maximum restriction, which means each subscriber account can only be accessed from exactly one registered device only.
    b) However, for the convenience of genuinely paying subscribers who might wish to access the paid site from more than one devices (e.g. at home, at work, mobile), the limit could be set to a more lenient number, such as "2" or "3".
3) Each user device must be registered or enrolled as an authorized device for a particular subscriber account.
    a) For maximum ease of deployment, device registration can be made automatic upon account login on first come first serve basis. For example, if the device limit is set to "2", the first two devices used to login using the account will be automatically registered as the authorized devices for this particular subscriber account.
    b) Other device registration options are available, such as registration via email link. However, it is not encouraged.
4) Every time when a user logs in, provided that the login ID and password are correct, the device used to log in will be automatically verified in the background without any additional user steps for maximum transparency and minimum disruption of user experience.
    a) If the device is verified to be a registered device for the subscriber account, the user will be granted access to the paid content.
    b) However, if the device is not a registered device, the system will quickly check if the device limit has been exceeded for this account. If not yet exceeded, this new device will automatically be registered as an authorized device.
    c) Otherwise, if the device limit has been exceeded, access to the paid content will be disallowed. A customizable message will be prompted to user to indicate that the device limit has been exceeded. (Very much like how the user is notified when the maximum number of simultaneous sessions has been exceeded.)

2.6 Comparison

	TheGRID	**Hardware OTP Token**	**USB Dongle**
Effectiveness			
Make account sharing difficult	Yes	Yes	Yes
Difficulty to share account	High (Requires re-registration)	Low (Token code can be shared over the phone)	High (Difficult to share)
Ease of Use (End User)			
User action required during login access	None	Enter token code	Plug in dongle
First time installation	Registration only	Registration only	Software installation and registration
Ease of Deployment			
New Hardware	Auth Server	Auth Server, tokens	Auth Server, USB dongles
Physical Delivery	None	Delivery of tokens by courier service	Delivery of dongles by courier service
Speed of deployment to millions of users	Immediate, over the web	A few weeks	A few weeks
Cost			
Initial Costs	Licensing, Servers, Implementation	Licensing, Servers, Implementation, User Tokens	Licensing, Servers, Implementation, Dongles
Operation / Maintenance Costs	Servers	Servers, Tokens	Servers, Dongles
Additional Growth Costs	Licensing	Licensing, Tokens	Licensing, Dongles

Contact Information

Company	e-Lock Corporation Sdn Bhd
Address	Business Suite, 19A-26-3A, Level 26, UOA Centre 19 Jalan Pinang, 50450 Kuala Lumpur, Malaysia.
Phone Fax Website Email	+ 60 3 2166 2981 + 60 3 2166 2982 http://www.elock.com.my/ info@elock.com.my