



WHITE PAPER

Entitlement Management Server

Presented by:

Amir A. Khosrodad

August 2007

For more information, please contact us at

Cranium Softworks
8070 Georgia Avenue
Suite 305
Silver Spring, Maryland 20901

(301) 589-8930 Tel.
(301) 589-8932 Fax.

info@craniumsoftworks.com

www.craniumsoftworks.com

Table of Contents

Table of Contents 2

Executive Summary 3

Introduction 4

The Fundamental Problem 4

Introducing Entitlement Management Server (EMS) 5

How EMS Works 5

How EMS Can Help You 7

Executive Summary

Username and passwords are often necessary to access online information or services that require membership or a paid subscription to the site. Today, virtually all organizations that need Membership Services rely on some type of security mechanism to authenticate their member users. Over the years, technological advances in encryption, validation, and Directory Services have made today's security engines extremely powerful, yet the concept of applying a security solution for the purpose of enforcing entitlements suffers from a fundamental flaw in its logic: the assumption that the user will keep his credentials private and secure. That is because, in certain situations, such as an online subscription to a website, once the user has created an account, there is no real incentive for him to keep his username and password a secret. Stolen or shared user credentials constitutes almost 99% of all unauthorized traffic on such websites, translating to millions of dollars worth of lost revenue for the online organizations.

The Entitlement Management Server (EMS) is a powerful platform that works in conjunction with a site's security engine to deter and minimize entitlement misuse of membership-controlled content. Under EMS' electronic "license" model, there can only be one active license certificate per account such that if another user logs into the system with the shared credentials, the active certificate is passed on to him disabling entitlements for the original account owner. Hence where there was no incentive for users to keep their credentials un-compromised, Entitlement Management Server provides that incentive in a simple, efficient and effective manner with virtually no impact on user experience or convenience. In a nutshell, EMS creates a disadvantage for the users attempting to share their usernames and passwords.

Introduction

Over the last few years, the Internet has rapidly evolved into a principal medium for communication, commerce and collaboration. To support their business models and their operational processes, more and more organizations have been restricting portions of their websites to a select number of users that, in one way or another, have paid for this privileged access. An online publication, for example, may restrict its premium content by requiring users to pay a subscription or membership fee before access is granted. Today, virtually all organizations that require Membership Services rely on some type of security mechanism to authenticate their users. Online publications, web-based applications, even dial-up Internet Service Providers (ISPs) often utilize a "Username / Password" scheme to try and make sure that only those users that have paid for and are "entitled" to access the site are granted admission. But where a "security" restriction paradigm is appropriate for an online banking system, its application and effectiveness to secure a subscription or membership service is questionable.

The problem that most – if not all – these Internet vendors are facing, is that no matter how secure an authentication mechanism they deploy, and regardless of how much time and money they spend on enhancing their security infrastructure, they seem to be losing larger and larger revenue and market share as a result of unauthorized usage. Surprisingly, only about one percent of unauthorized usage on these systems can be attributed to hackers or those with a technological method of circumventing the site security. From a statistical perspective, virtually all unauthorized traffic on the majority of these sites comes from stolen or shared credentials.

The Fundamental Problem

The inherent problem with using authentication and authorization schemes to enforce entitlements, stems from the basic (and often misunderstood) difference between the purpose of security versus that of entitlement management. Security, by its very nature, attempts to authenticate a user with the assumption that only the valid user would have the correct set of credentials. This mechanism is, for the most part, effective where the user has a significant stake in keeping his credentials secure. On an online banking system, for example, it is to the user's advantage to maintain the secrecy of his username and passwords. Hence the intent of security is to protect both the system as well as the user, such that both parties benefit from this protection.

However, the user side of this "benefit" is precariously missing in certain scenarios such as subscription to an online publication, as mentioned earlier. In that case, once the user has paid for his subscription fee and has a valid account on the website, there is virtually no incentive for him to keep his username and password private. Any number of people may access the account through his credentials without any cost or inconvenience to the valid account owner. He may let friends, family members and co-worker use his credentials to access the site. In more extreme cases, he may even post his credentials on public bulletin boards or even sell his credentials to multiple unauthorized users resulting in significant losses to the organization. The bottom-line seems to be, that if a user willingly or accidentally shares his username and password with others, there is no viable technological way of distinguishing between the authorized users and the impostors, and therefore, no way of meaningfully managing entitlements... at least until now.

Introducing Entitlement Management Server (EMS)

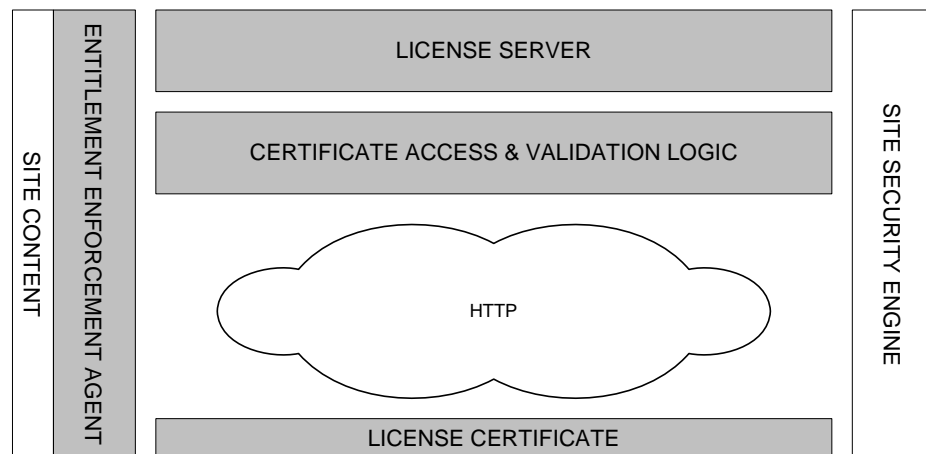
The Entitlement Management Server (EMS) was developed by Cranium Softworks with the simple understanding that security and entitlement enforcement are not necessarily the same. Where there are no incentives for users to keep their account credentials private, the assumption must be that users will inevitably compromise their passwords. As such, the aim of EMS is to provide the incentive for account owners not to share their account information. *It is important to note that EMS does NOT prevent users from sharing their credentials. Rather, it creates a disadvantage for users who do.* Perhaps, a more accurate description of EMS would be that it provides a detriment to users who share their passwords by disabling their entitlements if a violation is detected.

Based on an electronic “license” model, EMS associates a user’s credentials with an electronic certificate that is issued to the user during a successful login. The login procedure can still be handled through a traditional username/password security engine, however, access to the site depends on the existence and validation of the user’s electronic license. So long as the user has a valid and active license certificate, access to the site is granted. However, since there can only be one active certificate per account, if another user logs into the system with the same credentials, the active certificate is passed on to him disabling entitlements for the original account owner.

Again, it is important to re-iterate that EMS does not prevent sharing of usernames and passwords, but because under an EMS-controlled environment, the account owner would lose his privileges if his credentials were compromised, it would be to his advantage to protect the privacy of his username and password. In short, EMS is a true entitlement management system that works in conjunction with the site security engine to effectively deter and minimize entitlement misuse on any distributed system.

How EMS Works

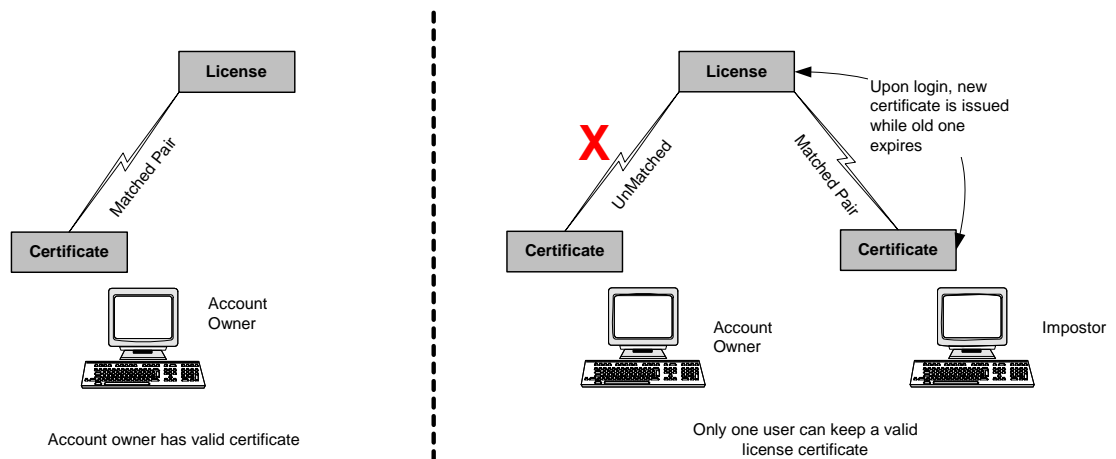
Based on a 3-tiered architecture, EMS is comprised of the following components.



The License Server is a database that contains all user licenses along with an associative field that identifies the users' security engine records. Upon a successful login, a certificate is created by the Access and Validation layer and assigned to the user. This process is transparent to the user.

As the user logs into the EMS-protected website, the certificate's validity is checked by the Entitlement Enforcement Agent against the License Server before access is granted to the requested site content. If the license record does not entitle the user to the requested content then access is denied. What's more, the license server can be configured to handle multiple types of licenses each with a different level of access to the site.

If the account owner's credentials are used by another person (on another computer) to log into the site, the Certificate Access & Validation layer checks for a successful authentication by the security engine and a new certificate is generated and sent to the new client. The License Server would then automatically expire the original certificate, which makes the account owner's license invalid while the new user becomes the active user.



Theoretically, users could still share access to the site by alternating logins between them, but because each content page on the site requires a valid certificate, the users are forced to login with every click. To protect against alternating logins, several configuration mechanisms can be considered. The login procedure could be lengthened to make alternating logins very inconvenient. Or limits can be set on the License Server as to how many times a user can be issued a new certificate within a given period of time. Moreover, programmatic triggers can be set up to perform various functions if an account reaches that limit.

Although on the surface, the EMS model would seem to "lock" the user to a single computer, in fact the account owner is free to access the site from any connected machine on the web. He would simply log into the site and automatically obtain a new certificate for the computer he is on. However, doing so automatically expires the certificate on the previous computer he used. If necessary, the number of times that a user can move from one computer to the next can be controlled by the entitlement policy of the site.

How EMS Can Help You

The Entitlement Management Server is an extremely flexible tool that can be deployed in a number of different environments and configured to support almost any distributed business model.

Membership Account Integrity Enforcement

As described in this white paper, membership account integrity enforcement is the principle purpose of EMS. Content libraries, online subscription services, dialup internet service providers or any website that requires payment for access can expect significant savings in revenue that would otherwise be lost to multiple users sharing a single account. EMS' flexible configuration capabilities would allow organizations to enforce custom account-integrity policies by defining how EMS should handle violations. These policies can range from limiting the number of certificates issued per given time period, all the way to simply raising a warning message about the violation.

Offer Additional Licensing Schemes

Today, many online subscription services provide broad institutional site license agreements that are usually enforced by IP Address filtering. That means that any user within the client's network can have unlimited access to the site. EMS provides the online vendors and publishers the ability to limit the scope of their site license agreements by establishing a Per-Seat licensing scheme. Client users would still be authenticated using their IP address. However, EMS can control the number of licensees that would be available for the institutional client. This way, the client only purchases the number of seats it needs with the option to increase or decrease that number at any time.

Digital Rights Management

Copyright enforcement over the web has been a subject of great controversy over the last few years. Electronic publications, research firms, news and periodical archives, online databases and virtually any organization that produces premium (for-pay) content over the internet currently does so accepting copyright violations as a natural expense of doing business over the web. For such companies, EMS can easily integrate with Cranium Softworks' Java based Content Viewer to stop copyright violations with little or no impact on the user's online experience. The combined integrated solution provides unparalleled Digital Rights Management (DRM) capability that keeps users from saving, emailing, copy/pasting or even printing the content while protecting accounts from shared or stolen credentials.

Software Client Access License Enforcement

Software, by its very nature, is intangible and non-physical; it can easily be copied, distributed, and re-used. That means once purchased, the new owner can distribute or sell a copy of the product without losing ownership of the original. With the advent of the Internet as a model for distributing applications and the evolution of delivery mediums such as Application Service Providers (ASP), enforcing software license entitlements has become an almost impossible task. The EMS solution provides for a secure and dependable method of ensuring software license integrity. If the user installs or accesses the software from a different machine, the original license would, by default, become outdated as soon as the new license is used. This ensures a single seat usage of the software per each Client Access License (CAL). The EMS solution is simple, reliable, and easy to integrate into applications. Furthermore, a single License Server can be utilized to validate licenses for multiple applications residing within an environment.

Complying with all applicable copyright laws is the responsibility of the reader. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Cranium Softworks, Inc.

Cranium Softworks, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Cranium Softworks, Inc., the furnishing of this document does not give the reader any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Cranium Softworks, Inc. All rights reserved.

The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Microsoft Active Directory, is a registered trademark of Microsoft Corporation in the United States and/or other countries.