Aladdin.com

HASP® HL

REINVENTING SOFTWARE PROTECTION & LICENSING

Software Protection: The Need, the Solutions, and the Rewards

White Paper for Software Publishers

Aladdin®

SECURING THE GLOBAL VILLAGE

Table of Contents

Intellectual Property @ Risk

Software piracy is the practice of copying and using a software product without the permission of its owner or developer. Although most computer users today are aware that unauthorized use and duplication of software is illegal, many still show a general disregard for the importance of treating software as valuable intellectual property.

Worldwide, there is a great deal of illegal software in current use. According to the IDC/BSA 2004 piracy study, nearly $29 billion annually is lost to software piracy worldwide. With the rapid adoption and use of broadband connectivity, peer-to-peer sharing and CD burners, protecting software revenues and intellectual property is more critical than ever.

75%of broadband users use P2P networks to share data.
Jupiter Media

Various categories of software piracy include:

- Soft-lifting: purchasing a single licensed copy of software and loading it onto several computers, contrary to the license terms. For example, sharing software with friends, co-workers and others.
- Uploading and downloading: making unauthorized copies of copyrighted software available to end users connected by modem to online service providers and/or the Internet.
- Software counterfeiting: illegally duplicating and selling copyrighted software in a form designed to make it appear legitimate.
- OEM unbundling: selling standalone software that was intended to be bundled with specific accompanying hardware.
- Hard disk loading: installing unauthorized copies of software onto the hard disks of personal computers, often as an incentive for the end user to buy the hardware from that particular hardware dealer.
- Renting: unauthorized selling of software for temporary use, like you would rent a video.

People who engage in software piracy fall into several categories:

- Dealers selling hardware pre-loaded with illegal software
- User organizations making unauthorized copies of software for internal use
- "Professional" software counterfeiters
- Competitors using unauthorized software copies to develop competing products
- Hacker web sites offering illegal software to users
- Any individual who makes an unauthorized copy of someone else's software program

Software piracy impacts all aspects of industry: accounting, financial, education, automotive, aerospace/defense, gaming, gambling, medical/healthcare, manufacturing, multimedia, telecom, transportation, and engineering, to name a few. Thus it comes as little surprise that more and more businesses are looking for ways to protect their software and intellectual property.

According to figures supplied by the BSA, engineering software publishers could increase revenues from software in use by up to 37% by proactively combating software piracy. Similar to the engineering industry, other software publishers can get more business from their existing customers and see an increase in the number of seats sold per site by taking appropriate measures to safeguard their products.

For every two dollars of legally purchased software, one dollar was illegally obtained.
2004 BSA & IDC Global Piracy Study

The Answer—Software Protection

The term software protection is used to describe all the methods that a software publisher can use to ensure that users can run only those copies of software that have been legally purchased. It is important to note that there is no such thing as a perfect software protection mechanism. Ultimately, if someone wants to use your software illegally, they will find a way. The aim of software protection, then, is to make the effort of illegally running a program more expensive than a license to run the program.

So while the direct objective of software protection has always been of a preventive nature, today the quality of software protection is also measured by the broadness of the solution and its ability to answer further software commerce needs. A good software protection solution will not only enable software publishers to increase their revenues, but also gain remote control over their software and its distribution and channel management. It should also enable innovative sales opportunities and flexible licensing capabilities, which give publishers the freedom to concentrate on doing business without the worries of license violations.

Furthermore, since a software protection system is incorporated into the publisher's product, it carries with it logistical and commercial issues that affects their entire organization: from the engineering team that is responsible to implement and test the solution, to the product management team that makes commercial decisions, and through the ordering and shipping departments. A good software protection solution addresses these issues and provides the flexibility required by all these areas in the publisher's organization.

Software Protection Methods

Two major forms of control mechanisms can be used to create the incentives for obtaining the software legally and penalties or disincentives for using the software illegally:

Legal and Marketing Control Mechanisms

Software license agreements and copyright law are being used to prevent software piracy. Of the two legal control mechanisms, copyright law is the more important, covering all software automatically. These control mechanisms do not prevent a user from inadvertently or intentionally copying the unauthorized software. The power of these mechanisms is in the legal remedies available to the software suppliers against software piracy.

Software publishers and suppliers are also using various marketing and educational control mechanisms to reduce the incidence of software piracy. For

example, these include volume discounting, site licensing, strong focus on customer support, teaching that software theft is wrong, etc. While this form of control may prevent accidental use of unauthorized software by the end user, it will not prevent those who engage in software piracy.

As a result, you should adopt both marketing and legal measures, realizing that they help reduce casual or inadvertent piracy but will not stop more sophisticated, direct piracy efforts.

Hardware-based copy protection systems offer the best, most proactive solution for software publishers.

Technology-Based Control Mechanisms

Technology-based control mechanisms include all programs and devices that prevent the unauthorized use of software. This form of protection delivers a solid value proposition that, unlike legal mechanisms, cannot simply be ignored. In addition, it is more cost-effective to enforce than litigation.

Technological mechanisms use an encryption process or other protective measures to protect the software. The most common approaches are: making distribution disks copy resistant, access locks, hard-coded numbers in computer memory, software resident inside a ROM chip and copy protection security devices, also known as dongles. This form of control will prevent accidental use of unauthorized software by the end user. In some cases these methods will also prevent attacks of software piracy, depending on the strength of the control mechanism.

Technological protection comes in two forms: software and hardware, the latter being a much stronger mechanism, aimed at combating software piracy. Today, software-based copy-protection is associated with license management systems and license files. The strength of these systems however, is in their licensing capabilities. The fact is that many software-based copy protection publishers offer a hardware-based copy-protection key when it comes to enhancing the protection level of their software application.

Hardware-Based Software Protection Keys

Hardware-based copy protection systems offer the best, most proactive solution for software publishers. These systems offer the most secure solution while placing a minimum burden, if any at all, on the software user. There are two major types of hardware-based solutions which differ in strength: EEPROMs and the much stronger ASIC-based or microcontroller-based solutions.

Electrical Erasable Programmable Read-Only Memory (EEPROM) is a standard memory chip that can be purchased off the shelf. Dongle publishers that use these chips will often mask them in an attempt to physically conceal their identity and the known technology. EEPROM contents are almost always readable via software and they generally contain plain data that make it possible to emulate the process with a software patch.

EEPROM-based copy-protection keys are "dumb" devices that let you store data. This is because validating the presence of the device in order to determine whether the user is authorized is summed up in a simple operation of just reading what is stored on the EEPROM and comparing it to an expected value.

Intelligent Devices

Application Specific Integrated Circuit (ASIC) is a chip designed for a special application and cannot be purchased from just any electronics store. An ASIC can be pre-manufactured for a special application or it can be custom manufactured (typically using components from a "building block" library of components) for a particular customer application. This is an extremely secure technology because only the company that designed and manufactured it knows the technology. Microcontrollers also fall under this category.

Both ASIC-based and microcontroller-based keys are referred to as "intelligent" devices because they can deploy encryption. ASICs have an on-chip encryption engine designed within their logic. Microcontrollers activate an encryption algorithm that is burned into an internal EEPROM.

Protecting software with a hardware-based key is the best way to validate that a user is legally using the application.

Encryption—the Heart of Software Protection

The best way to validate that a user is legally using a software application is to protect it with a hardware-based key and to verify that the key is connected to the user's computer during the application's runtime. There are two ways to perform the verification:

- Send the key a query and check the response; if the response is as expected, then the key is present. This approach is fundamentally insecure. Checking for an expected response can be easily hacked and removed – leaving the application lacking protection.
- The other, most secure, method is to "use" the key (as opposed to checking it) to decrypt encrypted strings or text and to deploy those within the application. As a result the application will run properly, if at all, only when the strings will be decrypted properly i.e. when the right key is connected to the computer.

Any method of encrypting text is referred to as a cipher. The resulting encrypted text is referred to as ciphertext. Some ciphers work by simply realigning the alphabet (for example, A is represented by F, B is represented by G, and so forth) or otherwise manipulating the text in some consistent pattern. However, almost all serious ciphers use both a key, which is a variable that is combined in some way with the unencrypted text, and an algorithm, which is a formula for combining the key with the text. There are two categories of ciphers: stream and block.

Stream Cipher

A stream cipher is a method of encrypting text in which a cryptographic key and an algorithm are applied to each binary digit in a data stream, one bit at a time. This method is not used much in modern cryptography.

Block Cipher

Another method, used much more frequently, is the block cipher. A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block

of data at once (as a group rather than to one bit at a time) into a block of ciphertext (encrypted text) data of the same length. This transformation takes place under the action of a user-provided secret key. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key.

Cipher Block Chaining

Associated with block ciphers are cryptographic modes, which combine the basic cipher, some sort of feedback, and some simple operations. One mode of operation for a block cipher is the cipher block chaining (CBC) mode. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block.

HASP® HL—Not Just Any Hardware

The price of software reflects the time, resources and efforts publishers put into delivering a working tool for their customers, tools that comply with their expertise and skills and is most suitable to answering their needs. Expensive software is a target for software piracy, which results in the sale of applications for a fraction of their cost. It is in the best interest of every software publisher not only to protect their intellectual property, but to protect it with the most secure mechanisms.

Typically one of the most difficult challenges dongle manufacturers are faced with is remaining one step ahead of people who engage in software piracy. To achieve this, Aladdin engineers regularly enhance and upgrade our hardware and software security products. HASP HL is the most recent improvement.

A technological leap from its predecessors, HASP3 and HASP4, HASP HL provides a superior method of encryption with an algorithm that is burned into the hardware.

HASP HL incorporates an advanced microcontroller onto which the encryption algorithm and a 128-bit encryption key are indelibly burnt. This unique technology prevents reverse engineering and foils even the most determined hackers.

HASP HL uses the 128-bit AES (Advanced Encryption Standard) algorithm. AES is a conventional block cipher. It was chosen in October 2000 by The National Institute of Standards and Technology (NIST), as a DES replacement, for the US Government's general use. AES is based on the Rijndael algorithm, which was invented by Joan Daemen and Vincent Rijmen. The strengths of Rijndael are: simple and elegant design, efficient and fast on modern processors, and compact in hardware. This makes AES suitable for a broad range of applications.

During runtime HASP HL receives encrypted data from the protected application and decrypts it in a way that cannot be imitated. The decrypted data that is returned from the key is deployed in the protected application so that it affects the mode in which the program executes: it may load and run, it may execute only certain modules or components, or it may not execute at all.

The global piracy rate currently stands at 36%.
2004 BSA & IDC Global Piracy Study

HASP HL technology is based on the most advanced anti-hacking mechanisms, which are virtually impossible to crack. Furthermore, HASP HL features pseudo-random encryption of all communication between its various system components: the HASP HL hardware, the HASP HL Device Driver, and the HASP HL API. Communication encryption prevents emulation of the key, which is one hacking method used in software piracy.

HASP HL copy protection keys contain internal memory with up to 4 Kilobytes that can be written and read in the field. Other types of HASP keys contain a real-time clock that measures time and date. The HASP memory chip provides a vault for safekeeping data. The memory and the internal clock also provide a means of implementing new and diverse sales opportunities.

Enabling Secure Business

Publishers cannot afford to have their distribution channels violate the product protection or their licensing terms.

Security and protection do not end with encryption. There are other aspects that need to be considered. With today's competitive, fast-paced market, the ability of software publishers to be first in delivering their solution to end users may mean the difference between selling to customers or losing them. But not only do publishers need to reach their customers quickly; their products need to reach their destination securely. Publishers cannot afford to have their distribution channels violate the product protection or their licensing terms.

The HASP HL family of keys supports innovative marketing techniques specially designed to help software publishers reach their customers quickly and securely and to enrich their sales process in general. One of the current trends in the industry is the increased availability of component-based software. Selling component-based software means that there is a need to distribute and license separate software components or modules. In one key, HASP HL protects and licenses multiple products, design modules, add-ons and plug-ins. It can secure modules separately and enforce pre-determined licensing terms for each one. Some software publishers using HASP HL securely store licensing terms for more than 400 software modules in its memory. This, plus the fact that the HASP HL memory can be updated remotely, gives them the freedom to concentrate on doing business without the worries of license violations.

Here are some of the business models software publishers can implement with HASP HL:

- Evaluation model – enable the activation of software a limited number of times
- Demo model – supply a "lite" version of the software by enabling the activation of a limited number of features
- Subscription model – allow periodic software activations
- Try-before-you-buy – limit software activation by time
- Pay-per-use – charge for specific features and activations
- Rental model – rent parts or all of the software
- Floating model – charge according to the number of users activating the application in a network

Furthermore, HASP HL enables publishers to quickly upgrade their customers'

software by remotely updating their HASP HL keys. In general, end-users upgrade their software by directly contacting the publisher, or a reseller. HASP HL is extremely flexible with its open memory architecture enabling secure channel management; publishers can entrust field upgrades and licensing to their resellers and distributors.

Protect Once – Deliver Many™

The implementation of software protection has historically been tied to licensing; every time the software's licensing model was changed, the security would have to change also. HASP HL breaks that paradigm with a "Protect Once – Deliver Many™" model. Implementation of software protection is performed only once, while commercial decisions can be taken later, and licensing models can be implemented or changed without affecting the product's security. This reduces the software publishers' time-to-market and significantly enhances their flexibility and freedom in defining new sales and licensing models.

Portable Security for Any Computer

Good dongle manufacturers must keep up with new technologies, ensure that products meet the demands of customers, and meet the demands of end users by supporting the platforms and protocols of the modern PC user.

All PCs, laptops, and Apple computers available on the market today have USB ports as a standard feature. This is the first time PC and Mac computers have come together in harmony on a hardware standard. We are looking forward to a future of hybrid peripherals of a cross-platform nature, which, until now, has been limited to software applications.

In 1998, Aladdin released USB keys with the most compact design and a rich host of advantages. In 2000, HASP4 USB was released – a new generation USB version of the HASP4 key – which clearly set a new performance standard. To meet the emerging need for cross-platform protection, in 2001, the HASP4 USB Cross-platform solution was introduced.

And in September 2004, Aladdin announced HASP HL, the next generation in hardware-based software protection. This USB key is platform independent, supporting both PCs and Macs (Windows, Mac OS and Linux) – a feature made possible only with the introduction of USB and its total integration by the leading computer manufacturers.

According to IDC, electronic licenses will grow to 83.2 % of worldwide end-user software spending through 2007.
Worldwide and North American Software Sales Forecast, 2002-2007

HASP® HL in the Internet Age

The pervasive nature of the Internet has struck at the core of traditional business models and practices, requiring open, flexible and responsive solutions. Using the Internet to distribute software puts an end to lost or damaged goods and late deliveries. ISVs can save thousands of dollars on media, shipping, and labor costs and on storage space, thus eliminating administrative headaches. For software commerce the Internet allows customers to get products more quickly and in higher volumes, easing the strain on human resources and reducing labor costs. HASP HL complements Internet-driven software sales with greater security.

Although hardware-based, HASP HL is a convenient solution for protecting applications and distributing them over the Internet. This is especially the case for software publishers that:

- Sell professional applications at extremely high prices – these require ample protection that only a hardware-based solution can provide.
- Sell applications that may not be suitable for Internet download and must be shipped shrink-wrapped to first-time users.
- Electronically distribute their products for immediate trial-only use and then provide the HASP HL key with the full purchased product

Once the application is in the field, software commerce can take its course via the Internet, boosted by the remote upgrading and licensing capabilities of HASP HL. Publishers can electronically ship software upgrades and additional components or modules, in conjunction with their licenses – to be safely stored in the HASP HL memory.

About Aladdin Knowledge Systems

Since 1985, Aladdin Knowledge Systems (Nasdaq: ALDN) has been at the forefront of the Software DRM (Digital Rights Management) and Enterprise Security fields. Proven technology has translated into solid, value-added and cost-reducing security solutions for both software publishers and enterprise security professionals. Aladdin's reputation is built upon a comprehensive line of products fulfilling the security needs of businesses operating in a world where quick and easy information accessibility is not only an asset, but also a potential risk. These products include eToken™, the next generation authentication key; the HASP® family of software Digital Rights Management solutions; and eSafe®, integrated content security.

With offices in nine international locations and a global network of resellers and distributors, Aladdin supports over 30,000 customers in 100 countries. Aladdin customers range from Fortune 100 corporations to financial, education and government organizations. The Internet and software security fields are continually evolving, and Aladdin remains committed to not only keeping pace, but leading the way, providing our customers with the most advanced security products on the market.

To learn more, visit the Aladdin web site at www.Aladdin.com

Printed in Israel
05827

Aladdin
SECURING THE GLOBAL VILLAGE

For more contact information, visit: **www.Aladdin.com/contact**

North America	T: 1-800-562-2543, 1-847-818-3800	F: 1-847-818-3810
International	T: +972-3-636-2222	F: +972-3-537-5796
UK	T: +44-1753-622266	F: +44-1753-622262
Germany	T: +49-89-89-42-21-0	F: +49-89-89-42-21-40
Benelux	T: +31-30-688-0800	F: +31-30-688-0700
France	T: +33-1-41-37-70-30	F: +33-1-41-37-70-39
Spain	T: +34-91-375-99-00	F: +34-91-754-26-71
Israel	T: +972-3-636-2222	F: +972-3-537-5796
Asia Pacific	T: +852-2166-8605	F: +852-2166-8999
Japan	T: +81-426-60-7191	F: +81-426-60-7194