SOFTWARE DEVELOPMENT
SD Times
The Industry Newspaper for Software Development Managers

Software Piracy: A Growing Problem

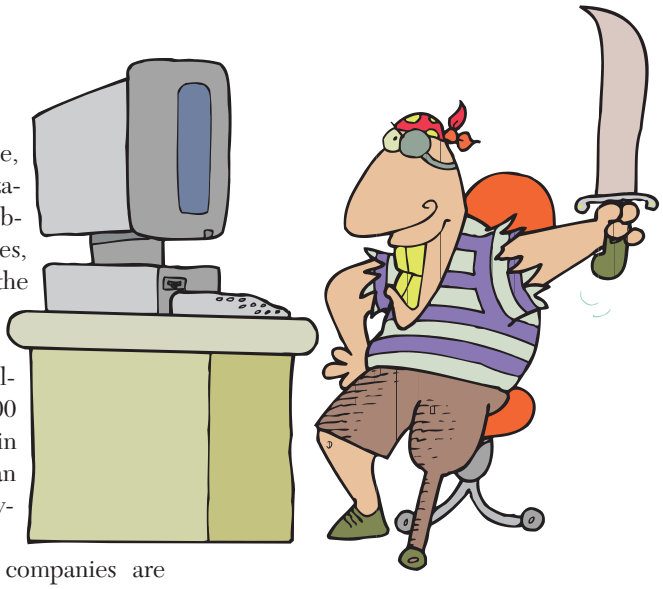
Licensing and security vendors admit there is no silver bullet to protect your intellectual property

BY LISA MORGAN

In 2004, a number of software companies are going to learn an expensive lesson the hard way: Hope is an ineffective measure against software piracy.

Some software publishers have thus far failed to adopt software protection and licensing management solutions because they represent yet another expense, which results in a higher cost of goods sold and thus higher end-user pricing. Adding technology also can increase the complexity of software products, making them more difficult to use, which can and does infuriate end users. And, software protection and license management products may interfere with the operation and performance of the software products they are designed to protect.

On the other hand, software piracy is a growing problem that affects more than just the large companies with high-profile cases in federal court. According to the Business Software Alliance, a global nonprofit organization that helps to shape public policy and prosecute cases, 23 percent of software in the United States was pirated in the U.S. alone in 2002. That translates to US$2 billion in lost revenue, 105,000 fewer jobs, $5.3 billion in lost wages, and more than $1.4 billion in lost tax revenue, according to BSA.



Although brand-name companies are targets for highly organized bootlegging operations, even small companies and individual developers fall victim to software piracy. The difference is, the small companies are forced to go out of business faster.

SCOPE OF THE PROBLEM

Part of the difficulty is that software piracy itself is a misunderstood term—even vendors in the software licensing and security space do not necessarily agree on what types of software piracy are the biggest problems, or to what extent.

Mental images of Johnny Depp on the deck of a tall ship or bootleg software ninjas don't help. Software piracy is not limited to modern-day Robin Hoods or sweat-

shops in Kuala Lumpur. Sure, individual users share software, and organized crime rings are capitalizing on the manufacture and distribution of illegal software that is so well conceived that the products appear to be authentic. Pirated software users have been known to actually register fake licenses with brand-name manufacturers and get access to specially priced upgrades.

Most software piracy isn't that sensational, however, and it isn't quite as malicious. Companies sometimes purchase stand-alone products and place them on servers or otherwise distribute more seats than they purchased. In some cases, companies fail to keep track of their software licenses, which can result in misuse, albeit unwitting in some cases. And, of course, software administrators and individual end users commonly fail to read software license agreements before clicking the "I agree" icon, which legally binds them to the contract's terms.

Lack of knowledge or intent is not exactly synonymous with innocence, however. Whether a person or company intentionally or unintentionally uses, copies or distributes unauthorized copies of software, the result is the same. That person and the company she works for have violated federal law, which can result in criminal and/or civil liability.

MITIGATING THE PROBLEM

Software licensing and security vendors are quick to point out that there is no silver bullet that will protect a software company from software piracy absolutely. What they can do is make the process difficult enough that the offending party will have to invest considerable time and perhaps money attempting to decrypt files or otherwise "work around" software license management.

"You can curtail, discourage or reduce software piracy, but you can't completely prevent it," said Yanki Margalit, founder and CEO of Aladdin Knowledge Systems in Israel. "Software developers need to sell more than just software; they also need to sell locks and keys."

The locks and keys come in the form of hardware and software. Hardware "dongles" plug into a USB or serial port and provide copy protection. Software checks to see if the dongle is present before unlocking the application.

Software-based approaches range from simple product activation (such as typing the serial number printed on the outside of a jewel case into a field) to server-centric methods that authenticate users and the software they use on an ongoing basis.

Vendors do not necessarily agree about which approach is better. Some say dongles are more secure than their software counterparts. Other say that dongles are expensive to buy, expensive to inventory and maintain, easy to lose and easy to spoof using a mirror.

Software methods also can have their weaknesses, however. For example, simple software activation, which requires a user to type a serial number into a field, may allow a user to install the software on multiple stand-alone computers without being detected. Hardware profiling is one way to get around that, but if the user adds or deletes hardware, then the software may fail to activate.

Some software publishers bind software license agreements to software products to thwart unauthorized distribution. Users with a little programming expertise can sometimes change a single bit "authorizing" otherwise unauthorized installation. Then, of course, there are "crack" programs available online that enable users to get around a vendor's software security mechanisms or to download bootlegged copies of software.

To make software piracy a little more difficult, third-party vendors are responding with shell wrappers and APIs that provide varying degrees of protection. Wrapping is quick, easy and relatively cheap. The use of APIs requires more time and effort, which some users say is well spent. APIs allow software developers to encrypt different files, such as the software license, the user manual and different components of a software program, separately as opposed to hiding a key in a hidden file (which can be discovered). Clearly, APIs provide a more granular level of control than wrapping.

MORE THAN SOFTWARE PROTECTION

Aladdin and Rainbow Technologies Inc. point out that their API technologies not only allow companies to mitigate unauthorized software use and distribution, they also enable software publishers to explore new sales models, such as limited-use demos, subscriptions, transaction-based sales and product updates and upgrades.

The technology allows software publishers to control which users have access to which products or product features so, for example, a software company can send a demo product to a customer that can be transformed into a fully functional product. Alternatively, software publishers can turn features on and off, depending on what the customer is willing to pay for.

In other words, don't focus on the detriments of use restraint; focus on the positives of customer choice. But is that just vendor marketing hype, or are their customers and the end customers actually buying into the idea?

"It's a trade-off. [End] customers hate licensing and activation schemes," said Dan Appleman, architect at software protection company Desaware Inc. "The question is, how tight do you want to be?"

Appleman pointed out that tracking the use of software licenses is, in effect, spying on customers, which raises privacy issues. Nevertheless, software publishers want to prevent the bypassing of licensing one way or another but not all want to employ Draconian measures, which is why companies like Desaware offer flexible options that allow for varying degrees of software protection.

MORE THAN SOURCE CODE

Aladdin's security solution, HASP, is being used in the entertainment industry by Soundminer Inc., which provides a search engine for sound effects. Soundminer's customers include Skywalker Sound, Sony and Warner Brothers.

Soundminer is using the enveloping feature of HASP, which encrypts all binaries, including code and data. Without a hardware dongle, the data cannot be decrypted. If the dongle breaks or an unauthorized person uses it, Soundminer runs a check against the key's unique serial number and invalidates the key.

Justin Drury, partner and head of software development at Soundminer, said that a customer will spend thousands of dollars recording a unique sound (such as a "Star Wars" sound clip) that can otherwise be easily downloaded and distributed by a freelancer (the sound industry apparently uses a lot of freelancers).

Typically, a freelancer works at a number of studios, so hardware profiling or other mechanisms tying software to a specific computer or location does not work in that market. In response to the sound industry's unique requirements, Soundminer created a "freelance mode" that encrypts sound files, which can be decrypted from any location using a public/private key scheme.

To further mitigate unauthorized downloads, Soundminder keeps a log of all transfers. Whenever a file larger than 1GB is downloaded, the system automatically sends an alert to the administrator.

TO PROTECT OR NOT

Cost is one reason why a number of software companies have yet to adopt third-party software licensing and security products. Apparently, companies selling software products at more than $1,000 per seat are the most common adopters because it makes sense to spend some percentage of revenue or tens of dollars per license to protect millions of dollars of revenue. Not all software protection and licensing management products lend themselves to the low-end market, however. Some vendors offer pricing schemes that are based on some reasonable percentage of revenue, which allows the publishers of $9.95 software or games to protect their products as well.

Vendors and users point out that the cost of software protection shouldn't be the deciding factor. Software publishers need to consider opportunity costs—the revenue they would have realized if their software had not been illegally copied and distributed.

Then again, if a customer would not have purchased the product in the first place, then the software publisher arguably hasn't lost revenue. But in the eyes of the feds, that's beside the point. ▮

Since its founding in 1985, Aladdin Knowledge Systems (Nasdaq: ALDN) has been at the forefront of the software commerce and Internet security fields. Aladdin's reputation is built upon a comprehensive line of security solutions that meet the 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:

SECURE SOFTWARE COMMERCE

HASP

HASP (Hardware Against Software Piracy) is a hardware-based cross-platform software copy protection system that:

- Prevents unauthorized use of software applications
- Protects your software copyright and intellectual property
- Supports multiple software licensing models

The end-result is better control over who uses your software, which features they can use and safe revenue/market share expansion.

Privilege

Privilege is a revenue-enabling software security platform that lets you:

- Distribute secure software via CD, ESD, or peer-to-peer networks
- Protect software copyright and intellectual property
- Reduce distribution/operational costs
- Integrate with in-house or hosted Web stores and shopping carts

By protecting your software once, you securely bring it to the market across all your channels and gain confidence that you are protected against piracy, unauthorized use, and casual copying.

ENTERPRISE AND INTERNET SECURITY

eSafe

eSafe 4 is a gateway-based, integrated content security solution and service that:

- Proactively protects networks against viruses, worms, spam and non-productive content
- Enables real-time inspection of Internet traffic without reducing network performance
- Reduces the risk of P2P, IM, security exploits and blended threats
- Enables lower total cost of ownership with an integrated, modular design

eSafe and its fully integrated content security solution enables more network uptime, decrease cost of ownership, increases employee productivity and strengthens network security.

eToken

eToken is a USB-based smart card device for cost-effective strong authentication and eCommerce. It provides:

- Enhanced security and ensures safe information access
- Improved and cost effective password and ID management
- Secure mobility of digital credentials/certificates and keys

With a single eToken, businesses get a set of ready-to-use security solutions meeting all their authentication needs (web access, VPN access, and network logon), and providing laptop and file security.

Visit the Aladdin web site at www.eAladdin.com

Contact us:
International T: +972-3-6362222, F: + 972-3-5375796, Email: info@eAladdin.com
North America T: 1-800-562-2543, 1-847-818-3800, F: 1-847-818-3810, Email: info.us@eAladdin.com
UK T: +44-1753-622266, F: +44-1753-622262, Email: info.uk@eAladdin.com
Germany T: +49-89-89-42-21-0, F: +49-89-89-42-21-40, Email: info.de@eAladdin.com
Benelux T: +31-30-688-0800, F: +31-30-688-0700, Email: info.nl@eAladdin.com
France T: +33-1-41-37-70-30, F: +33-1-41-37-70-39, Email: info@Aladdin.fr
Israel T: +972-3-636-2222, F: +972-3-537-5796, Email: info@eAladdin.com
Japan T: +81-426-60-7191, F: +81-426-60-7194, Email: info@Aladdin.co.jp