Choosing a Best-in-Class Software Protection Solution

OVERVIEW

Piracy and copyright infringement is a global epidemic that denies software companies their rightful return on investment. Even companies with low piracy rates feel the effects on their revenues. This hurts not only software vendors, but honest paying customers who are often hit with higher prices to compensate for the revenue loss caused by piracy and license non-compliance. As the numbers of personal computers and Internet users grow, the incidence of software piracy is accelerating. According to the Second Annual Business Software Alliance (BSA) and IDC Global Software Piracy Study, published in May 2005, thirty-five percent of the software installed on personal computers worldwide was pirated, representing a loss of nearly $33 billion. In a highly competitive environment with increasing risks of revenue loss, software companies must find economical but reliable ways to control access to and obtain fair compensation for their products.

The software protection market provides a range of hardware and software products, varying in levels of security, to combat piracy. Choosing the right level of security depends on multiple factors including the sensitivity or the value of the application being protected and the likelihood of attack. Software-based solutions can be deployed to keep honest customers compliant with license terms. However, the environment in which the software operates cannot be considered entirely secure and therefore software-based solutions do not create an impenetrable defense against piracy attacks.

For these reasons, software developers with a need for high security or who sell high value software frequently chose to incorporate a strong level of protection. A high level of protection is most commonly achieved by using sophisticated mechanisms such as hardware keys. Hardware protection offers strong, physical security that is as visible and reassuring as a deadbolt on a door while requiring minimal handling, if any, on the part of the software user. In addition, hardware protection keys can provide a secure space where information or access to that information can be encrypted and concealed within the key providing another layer of security.

HOW TO CHOOSE THE RIGHT SOFTWARE PROTECTION SOLUTION

When choosing a protection solution, there are several important questions to consider:

- Will the solution fit my evolving business model?
- Will the solution provide positive return on investment (ROI)?
- Will implementing this solution delay my time-to-market?
- Will the solution provide adequate protection against piracy and non-compliance?

Evolving Business Models
Software developers are discovering that merely protecting assets against piracy is not enough to remain competitive. To grow business and increase revenue potential, software vendors must support new and innovative licensing models. Demonstration, subscription and pay-per-use models are replacing standard perpetual licensing models. By offering a flexible suite of licensing models, vendors can meet diverse customer needs and scale as their business evolves. Vendors may wish to remain competitive by maintaining the ability to upgrade or change licensing models as necessary without re-implementing security. The scalability of the hardware key will assist developers in accomplishing this objective.

Positive ROI
As the software development industry becomes increasingly competitive, there is constant pressure to reduce costs and improve ROI. With the cost of piracy at an all time high, the implementation of a hardware key solution can significantly improve revenues, but software vendors must be careful to choose a cost-effective solution. The total cost of ownership must be considered, meaning the total cost to obtain, integrate, deploy and manage a security solution. If a solution is reasonably priced, but excessively taxes development resources during implementation or requires excessive management post-deployment, positive ROI cannot be realized.

Time-to-Market
Getting products quickly to market is often a high priority for software vendors. Delays in deployment can be costly and reflect poorly on the software development team. Software protection is typically implemented at the end of the software development cycle, when pressure to get the product to market is highest. This forces developers to require a solution that can be implemented quickly without extensive training or programming. A robust set of developer tools can cut development time while increasing the functionality delivered.

Strong Security
Software developers require solutions that include the latest advances in security technology. Unfortunately security is not typically a software developer's core competency. Developers can benefit by relying on the expertise and advice of a trusted software protection vendor when determining which security features will protect their assets most effectively. Finding a respected and experienced software protection vendor allows software developers to focus on what they do best.

Of all the decision criteria, security and implementation are two of the most complex points to consider. The security of a protection solution is important because without adequate security, software vendors cannot fully realize the enhanced revenue streams enabled by deploying an anti-piracy solution. Equally important are new innovations in the area of ease of use and speed of implementation. Through these innovations, software developers can directly improve time-to-market while leveraging the new evolving business models and reducing the overall cost of implementing a software protection solution.

SECURE SOFTWARE PROTECTION CRITERIA

With so many competing technologies available on the market today, choosing the right security solution can be a complex and overwhelming

process. Software developers must weigh many factors when choosing a solution. One area of consideration is the level of expertise of the security vendor. The vendor must have the capability to deliver a best-of-breed solution that will meet both security and cost requirements and protect assets now and into the future.

Security Criteria Check List:

- ✓ Software protection vendor offers security expertise and has a strong history of producing quality products
- ✓ Hardware key uses industry tested, government-approved open standards for encryption
- ✓ Solution provides protection against known hacking threats

THE IMPORTANCE OF SECURITY EXPERTISE

Commercial software protection companies offer state-of-the-art solutions that are available off-the-shelf today. These solutions provide software vendors with the benefit of a proven, tested solution. Security is a moving target, therefore software protection vendors must remain ever vigilant and a step ahead of those intent on violating security mechanisms.

Because security is not one-size-fits-all, software developers can benefit by forging a relationship with a security vendor who can serve as a trusted advisor and help select an appropriate solution. The right solution will balance ROI with the level of protection provided against piracy. When choosing a security vendor, important considerations also include experience within the industry, product innovation, recognition as a trusted security provider, and a proven track record.

THE LATEST ADVANCES IN SECURITY TECHNOLOGY

Software protection keys utilize encryption to shield vital information from those who are trying to gain access illegally. Therefore, the strength of the encryption is vital to the security of the key. Software vendors should consider hardware keys that utilize the latest technology innovations when the sensitivity or value of information being protected is high and in cases where the threat of attack is substantial.

Although there are different methods of encryption available, the Advanced Encryption Standard (AES) is the preferred industry algorithm for advanced levels of data security. AES is a FIPS-approved symmetric algorithm selected by the National Institute of Standards and Technology (NIST). Because AES has faced intense public scrutiny and is not privately guarded, software developers can have increased confidence when using the algorithm. By using AES, software vendors can be assured their valuable data is encrypted with the most trusted and widely used algorithm in the information security market.

KNOWN SECURITY THREATS

With advances in computer technology and the cleverness of hackers, cases of piracy are escalating. Even with a hardware key solution in place, software vendors may fall victim to attacks because security is only as strong as its weakest link. Driver replacement or emulation, replay, and brute force attacks are a few of the most popular attacks. To protect against these

threats, software vendors must choose a solution that includes the latest innovations and defense mechanisms.

Driver Replacement or Emulation Attacks
Although a secure hardware key is a fundamental component of a strong software protection solution, it can be compromised if the method used to communicate to the hardware key is insecure. Drivers used to communicate between the application and hardware key are software based and could be susceptible to a man-in-the-middle attack in which the driver is replaced or emulated. Strong encryption provided by a driver that utilizes a digital signature offers the highest level of protection against this type of attack. A digital signature serves to authenticate the driver to the hardware key. If the driver is replaced, authentication will fail, and further communication is disabled, thereby preventing unauthorized use of the software application.

Replay Attacks
In a replay attack, the hacker monitors and copies communications as they flow between the hardware key and the application. The hacker then replays the communications to compromise the device and gain access illegally to the application. To protect against this type of attack, the hardware key must send random communications to the application so that the hacker cannot discern legitimate from illicit communications and therefore cannot use these communications to compromise the hardware key and gain access to the application.

Brute Force Attacks
A common threat to software security that requires very little skill and much computing power is a password-guessing attack known as a brute force attack. Each hardware key is protected by a password that is necessary to allow software developers to access and set configurations on the key. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers and symbols until the one correct combination that works to gain entry to the key is identified. By choosing strong passwords, developers can make it virtually impossible (requiring millions of computing years) for hackers to crack a password. A strong password is one that combines upper and lower case letters, numbers and symbols, and exceeds eight characters in length. A tamperproof element that locks the key after a defined number of incorrect password attempts can be added to provide further protection against brute force attacks.

These are just a few of the many known attacks and security issues that software vendors face when selecting a security solution. The strength of a security methodology is based upon its ability to protect against exposure to attack. As technology evolves, security features are challenged over time and new innovations are required to provide a stronger, more secure system that is resistant to attack. An experienced vendor with a proven track record can help software developers stay one step ahead of software pirates.

EASE OF USE AND SPEED OF IMPLEMENTATION CRITERIA

“Ease-of-use” is a good idea and a popular slogan that many companies use to market their security solutions. However, the true test of ease-of-use occurs during implementation. Because software protection is most commonly added at the end of the software development cycle, developers should look for a solution that can be implemented quickly without extensive training or programming requirements.

The implementation process typically consists of the following phases:

- Learning curve to understand APIs and architecture of the hardware device
- Unit testing and module integration
- Verification of the design

The ease with which developers can perform unit testing, module integration and design verification is greatly dependent upon the initial phase of implementation. Therefore developer tools that help simplify the integration processes and shorten the learning curve can greatly enhance ease-of-use throughout the software development cycle.

THE IMPORTANCE OF ADVANCED DEVELOPER TOOLS

A complex application programming interface (API) that is difficult to use and offers inadequate functionality can cause unexpected delays in all phases of the implementation. Incomplete or poorly written documentation and a lack of samples or tutorials can further exacerbate the experience. Requiring developers to become fully immersed and knowledgeable of the technical details of a security solution unnecessarily increases the time to implement and the possibility of programming errors.

Developers can benefit from a robust set of tools that serve to simplify the implementation of license models, security features, and memory allocation. Developer tools can be used so that the developer needs to perform only a limited number of programming entries. A high-level system that maps easily to an API can streamline deployment by using tools to implement numerous complex security and licensing operations. Without such developer tools, these operations would need to be designed and implemented individually within each application.

Lastly, advanced developer tools can integrate security into the application in such a way that the security elements do not need to be re-implemented if the license model is changed in the future.

CONCLUSION

With market competition and the cost of piracy escalating, software companies must find economical but reliable ways to control access to and obtain fair compensation for their products. Software developers must select a software protection solution that will give them a competitive edge in the industry. Some key criteria for making the selection are whether the solution will meet the needs of their evolving business model, deliver positive ROI, integrate smoothly and easily into the application, and provide reliable security.

Of all the decision criteria, security and implementation are two of the most difficult points to consider. The security strength of a software protection solution is a top concern for developers who want to defend against revenue erosion due to piracy. Equally important are improvements in ease of use and speed of implementation that can directly improve time-to-market and reduce the overall cost of implementing a software protection solution.

SafeNet Overview

SafeNet (NASDAQ: SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit *www.safenet-inc.com*.

w w w . s a f e n e t - i n c . c o m

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** email: ***info@safenet-inc.com***

Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail *info@safenet-inc.com*
Website *www.safenet-inc.com*

Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538
Japan +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts)
+1 978.539.4800
U.S. (Minnesota)
+1 952.890.6850
U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)
+1 949.450.7300
U.S. (San Jose, California)
+1 408.452.7651
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers located worldwide.