Curtailing the Piracy Epidemic

A Case for Hardware Security Keys

OVERVIEW

Software is one of the most profound technological developments of our time. Software applications help us run our businesses, governments, schools, and personal applications. Unfortunately, the ease with which software can be digitally duplicated has led to widespread piracy. Electronic pirates fit many descriptions: from an employee who illegally installs a copy of an application on his or her personal computer to international software cartels that sell counterfeit software over the Internet. As computer usage grows, so does the potential for software piracy.

THE PIRACY EPIDEMIC

Software piracy in the U.S. and abroad is occurring at a staggering rate. To put some perspective on the problem, consider Wal-Mart, the world's largest retailer. If Wal-Mart experienced the same theft level that occurs in the U.S. software industry, literally one in four of their U.S. stores (431 to be precise) would be empty all the time – and not due to sales demand. To think of it on another level, imagine if every Wal-Mart store in every western and southern coastal state in the U.S. was always empty purely because of theft. With that level of loss, Wal-Mart would surely need to close its doors permanently or resort to military levels of defense to protect its inventory. The problem is even worse when we consider countries like Russia and China where less than 10 percent of all software is legally purchased. Consider the following facts:

- In 2003, nearly $29 billion in software was pirated worldwide (Business Software Association).
- Microsoft found that 90 percent of its software sold at online auctions is counterfeit (Microsoft's Worldwide Anti-Piracy Group).
- Of 86 countries BSA and IDC examined, one in three had a piracy rate of 70 percent or more.
- The Canadian Alliance Against Software Threat (CAAST) estimates that the Canadian economy lost more than $457 million (Cdn) to software theft in 2001.

COMMERCIAL PACKAGED SOFTWARE PIRACY

The chart below shows piracy rates in a sampling of regions around the world. This chart only considers piracy of commercial packaged software that runs on personal computers (PCs). If entertainment piracy numbers were included, piracy losses would be much higher.

Region	Piracy Percent	Piracy Losses
U.S./ Canada	23%	$7.2 billion
Eastern Europe	71%	$2.1 billion
Latin America	63%	$1.3 billion
Middle East/ Africa	56%	$1 billion
Asia / Pacific	53%	$7.6 billion
Western Europe	36%	$9.6 billion
Globally	**36%**	**$28.8 billion**

Source: First Annual BSA and IDC Global Software Piracy Study, July 2004

THE BIG PICTURE: IMPLICATIONS OF PIRACY

If individuals and businesses around the world did not perceive software as valuable, piracy would not be such a major problem. Although software is considered functionally valuable, users of pirated software do not feel compelled to legally purchase the rights to use software. Software piracy causes many serious implications for developers as well as consumers, governments and nations. For example:

- High piracy rates reduce profits that might have gone into more research and development for software developers. If software publishers were compensated for all of the software that was deployed, they could recover their costs more quickly, allowing them to fund new product development faster, and increasing innovation in the marketplace.
- In an economic impact study conducted for BSA, IDC concluded that lowering piracy by 10 percentage points over four years would add more than 1 million new jobs and $400 billion in economic growth worldwide.
- A lack of sales can send a message that a particular software application was not a success, discouraging developers from creating new and improved applications and directly affecting creativity in the marketplace.
- Piracy impacts financial resources, putting many small developers out of business and making it difficult for new developers to survive.
- Local and national economies lose tax revenue from billions of dollars of software that would have been purchased legally.

SAMPLE REVENUE LOSS FOR TWO SOFTWARE DEVELOPERS

Clearly a problem exists, but what can be done? Is government enforcement the answer? Copyright laws vary significantly from one country to the next. Enforcing copyright violations worldwide is not realistic for most developers. To further illustrate this problem, let's examine how much revenue loss could be occurring by looking at two different hypothetical companies, one large and one small.

Large Company

ABC Software designs a popular application and expects to reach a sales objective of 200,000 units this year. Assuming that only the U.S. is targeted, consider the following hypothetical scenario:

Item	Unit Cost	Notes
Software cost	$100	Includes overhead, development, testing and manufacturing
Packaging	$15	Software packaging and advertising
Distribution	$15	Shelf and distribution
Total cost	$130	
Resale price	$900	
Projected unit sales	200,000	
Projected total revenue	$180 million	
Projected net profit	$154 million	
U.S. piracy rate	22%	
Lost unit sales due to piracy	44,000	
Lost revenue	$39.6 million	
Actual profit	$120 million	
Lost profit	**$33.9 million**	

Based on projected sales of 200,000 units, it costs ABC Software $26 million to produce its software, grossing $180 million in revenues and netting $154 million in profit. Given the typical piracy rate in the U.S., ABC Software can expect that 22 percent of its installed base does not have legal rights to use the software. That pirated software represents a gross loss of $39.6 million or $33.9 million in profit.

Small Company

XYZ Software designs financial applications and expects to achieve a sales objective of 50,000 units this year. Assuming XYZ Software receives half of its sales from outside the U.S., consider the following hypothetical numbers:

Item	Unit Cost	Notes
Software cost	$35	Includes overhead, development, testing and manufacturing
Packaging	$10	Software packaging and advertising
Distribution	$10	Shelf and distribution
Total cost	$55	
Resale price	$350	
Projected unit sales	50,000	
Projected total revenue	$17.5 million	
Projected net profit	$14.8 million	
U.S. piracy rate	22%	
Average international piracy rate	36%	
Lost unit sales due to piracy in the U.S.	5,500	
Lost unit sales due to piracy outside the U.S.	9,000	
Total units lost to piracy	14,500	
Lost revenue	$5.1 million	
Actual profit	$10.5 million	
Lost profit	**$4.3 million**	

In this case, XYZ Software lost 14,500 units to piracy, costing the company $4.3 million in lost profit, or nearly a third of its possible profits.

Given both of these different scenarios, a significant amount of possible revenue and profit will be lost to piracy. These companies need a solution that will deter or eliminate piracy, thus increasing their revenue and profits. A hardware security key is just the solution to stop the piracy dilemma for these software companies and increase their profitability.

THE SECURITY KEY SOLUTION

Security keys are hardware-based products that must be present for security key-enabled applications to work. By adding a security key, piracy can be virtually eliminated by making digital copies of applications fully inoperable without a key. Because each key is unique, secure and extremely difficult to replicate, they provide an excellent deterrent to piracy.

Security keys increase the total cost of producing an application, but easily pay their way in captured sales revenues that would have otherwise been lost to piracy. Consider the previous examples of the large and small software developers with the added security of a hardware key.

Large Company

Item	Unit Cost	Notes
Software cost	$100	Includes overhead, development, testing and manufacturing
Packaging	$15	Software packaging and advertising
Distribution	$15	Shelf and distribution
Security key	$25	Assuming a discount based on volume
Total cost	$155	
Resale price	$900	Key cost absorbed in price
Actual unit sales	200,000	
Actual total revenue	$180 million	
Actual net profit	$149 million	
Increased total revenues	$39.6 million	Due to key
Increased net profit	$29 million	Due to key
Total cost of key	$5 million	
Return on investment	**578%**	

Small Company

Item	Unit Cost	Notes
Software cost	$35	Includes overhead, development, testing and manufacturing
Packaging	$10	Software packaging and advertising
Distribution	$10	Shelf and distribution
Security key	$35	
Total cost	$90	
Resale price	$399	Price raised to help offset key cost
Actual unit sales	50,000	
Actual total revenue	$20 million	
Actual net profit	$15.5 million	
Increased total revenues	$7.5 million	Due to key
Increased net profit	$5 million	Due to key
Total cost of key	$1.75 million	
Return on investment	**284%**	

In both of the above examples, net profit increased significantly by capturing lost sales due to piracy. The hardware security key can significantly increase profitability. Depending on the volume and profit margin built into the application, a security key can generate more than a fivefold return on investment.

More than 55 percent of all hardware keys used worldwide are SafeNet Sentinel keys. SafeNet's hardware keys use an encryption algorithm that is difficult to crack and is exportable outside the U.S.

BENEFITS OF SECURITY KEYS

In addition to curtailing piracy, hardware security keys provide other benefits, including:

- Increase revenue options with license management models such as software leasing or function-based licensing
- Promote customer satisfaction by ensuring that licensed users are receiving updates and product bulletins
- Protect against illegal licensing and distribution
- Promote secure relationships with channel partners
- Enable license compliance for clients
- Allow for secure demo licenses and remote software updating

THE SAFENET SOLUTION: THE SENTINEL® FAMILY OF HARDWARE KEYS

SafeNet's Sentinel family of hardware keys includes a complete line of full-featured, easy-to-use software protection solutions. Sentinel SuperPro secures more than half of the world's security-key enabled software. Developers rely on Sentinel products to increase their revenues, create demo limits, upgrade applications to fully licensed versions and provide software updating without the need to replace the security key.

HOW SENTINEL KEYS STOP PIRACY

SafeNet Sentinel keys use encryption algorithms to secure an application to a single machine. Using its algorithm, a Sentinel key passes an expected value from a query back to the software application. If the value is different from what was expected, the application will not function. The steps are as follows.

1. The Sentinel-protected application checks for the presence of the key. If the key is not present, the application will not function.
2. If the key is present, the application sends a time-stamped encrypted packet of information to the key. This information is essentially the application's way of testing the validity of the key.
3. The key decrypts the packet and returns another packet of information. The returned packet is the key's response or answer to the application.
4. The software ensures that the packet sent is the appropriate response and that the time-stamp is current. If the response is correct, the application is launched. If it is incorrect, the program is disabled.
5. The application continues to query the key every minute (or whatever you customize it to be), repeating steps 2 through 4 to verify that the key has not been removed. This makes sure that only a single key can be used for each application.

A Sentinel protected application sends a different test to the key each time it validates the application. Traditionally the application will have a minimum of 1,000 to 10,000 queries and expected responses to draw from at any given moment. For added security, half of the queries sent to a Sentinel key will be randomly generated and the response will be considered acceptable if it resides within the list of thousands of acceptable responses to the application. This added level of security counteracts record-and-playback hacks. In addition, the key is protected with up to 32-bit passwords and can be configured with multiple algorithms that make cracking the key even more difficult. The multiple algorithms can be cycled by the application, making it harder for a hacker to know which algorithm will be used at any given time.

The result of protecting an application with a Sentinel hardware key is reduced piracy. With a Sentinel hardware key, developers can recover profits lost to piracy, leading to greater revenues and dollars for future research and development.

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.