SafeNet
The Foundation of Internet Security

Curtailing the Piracy Epidemic: A Case for Hardware Security Keys

Software is one of the most sought-after 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

In the United States, 25 percent of all software is pirated. In countries like Russia and China, less than 10 percent of installed applications are legally purchased.

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 2001, $10.97 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).
- In the United Kingdom, a survey of corporate directors revealed that almost two thirds of companies contacted (60.3%) did not believe they had achieved 100% software compliance (Federation Against Software Theft, March 2002).
- According to the European Leisure Software Publishers Association (ELSPA), the UK video games industry loses £3 billion every year to piracy. In 80% of the raids carried out by

ELSPA, there is evidence of other criminal activity in addition to software piracy including drug trafficking, pornography and even terrorism. (5/2/2002)

- The Canadian Alliance Against Software Threat (CAAST) estimates that the Canadian economy lost more than $457 million (Cdn) to software theft in 2001.
- From the fall of 1999 to the spring of 2000, the sale of pirated software grew from 60 to 91 percent of all software offered at online auctions, resulting in more than 40,000 illegal auctions daily (SIIA, 2001).

Business Application Piracy

The chart below shows piracy rates in a sampling of countries and regions around the world. This chart only considers business application piracy. If educational and entertainment piracy numbers were included, piracy losses would be much higher.

Country / Region	Piracy Percent	Piracy Losses
U.S.	25%	$3.2 billion
China	91%	$645 million
Israel	44%	$72 million
South Africa	47%	$84 million
Russia	89%	$165 million
Germany	27%	$652 million
United Kingdom	26%	$679 million
Asia / Pacific	47%	$2.8 billion
Western Europe	34%	$3.6 billion
Globally	**36%**	**$12.1 billion**

Source: SIIA, 2001

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 research and development costs more quickly allowing them to fund new product development faster, and increasing innovation in the marketplace. 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 bring this problem home, 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 CAD 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	25%	
Lost unit sales due to piracy	50,000	
Lost revenue	$45 million	
Lost profit	**$38.5 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 25 percent of its installed base does not have legal rights to use the software. That pirated software represents a gross loss of $45 million or $38.5 million in profit.

Smaller 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	$14.75 million	
U.S. piracy rate	25%	
Average international piracy rate	36%	
Lost unit sales due to piracy in the U.S.	6,250	
Lost unit sales due to piracy outside the U.S.	9,000	
Total units lost to piracy	15,250	
Lost revenue	$5.3 million	
Lost profit	**$4.5 million**	

In this case, XYZ Software lost more than 15,000 units to piracy, costing the company $4.5 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

Hardware keys deter piracy by making illegal copies inoperable without the presence of a key.

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
Projected unit sales	250,000	Increased by 50,000 due to key
Projected total revenue	$225 million	
Projected net profit	$186.25 million	
Increased total revenues	$45 million	Due to key
Increased net profit	$32.25 million	Due to key
Total cost of key	$6.2 million	
Return on investment	**520%**	

Smaller 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
Projected unit sales	65,250	Increased by 15,250 due to key
Projected total revenue	$26 million	
Projected net profit	$20.2 million	
Increased total revenues	$8.5 million	Due to key
Increased net profit	$5.45 million	Due to key
Total cost of key	$2.3 million	
Return on investment	**236%**	

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.

Benefits of Security Keys

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

- Increases revenue options with license management models such as software leasing or function-based licensing
- Promotes customer satisfaction by ensuring that licensed users are receiving updates and product bulletins
- Protects developers against illegal licensing and distribution
- Promotes secure relationships with channel partners
- Enables license compliance for clients
- Allows for secure demo licenses and remote software updating

The Rainbow Solution: The Sentinel® Family of Hardware Keys

More than 55 percent of all hardware keys used worldwide are Rainbow Sentinel keys.

Rainbow's Sentinel family of hardware keys includes a complete line of full-featured, easy-to-use software protection solutions. Sentinel SuperPro, Rainbow's flagship security key, 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

Rainbow's hardware keys use a proprietary encryption algorithm that is difficult to crack and is exportable outside the U.S.

Rainbow Sentinel keys use a proprietary encryption algorithm to secure an application to a single machine. The algorithm is exportable outside the U.S. and is harder to crack because of its proprietary nature. 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, 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.

Sentinel keys verify the presence of the hardware key every minute using different queries.

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 outside the list of thousands of responses deemed acceptable 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™
The Foundation of Internet Security

www.safenet-inc.com

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

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
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 3 5719 2731
Japan(Tokyo)+81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794
Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
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. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers located worldwide.

©2004 SafeNet, Inc.