

If three years ago you had asked EDA-software vendors about software piracy, they would have answered, "It's not a big problem." The addition of licensing software, such as FlexLM from Macrovision, to their tools acted as a good enough deterrent "to keep an honest man honest," in the words of one vendor. Now, in the age of WANs (wide-area networks), developers working on designs worldwide and 24/7, and ever-more-rampant EDA-software legal disputes, legal land mines are cropping up as fast as the pirates are finding new ways to profit. Accordingly, EDA-software vendors are taking software protection more seriously, and so should you.

Inadvertent piracy or use of stolen tools can put you at as much legal risk as people who bootleg and sell stolen software as their "business." So, EDA-industry organization EDAC (Electronic Design Automation Consortium) and its members are getting tough and pursuing the pirates. And, EDA vendor Silvaco, which two years ago won its misappropriation-of-trade-secrets case against Circuit Semantics, is now going after customers. It is attempting to recover the license fees for its software plus a percentage of revenue generated from products that those Circuit Semantics customers originally developed with Silvaco's stolen software. Among Silvaco's targets are AMD and Intel.

GETTING SERIOUS ABOUT PIRACY

Increasing complaints from its member companies and China's greater role in electronics prompted EDAC this year to establish a committee to gauge whether EDA piracy is real or an urban legend. It found that the problem is real, growing, and could wreak havoc on the \$3.5 billion EDA market, according to Laurence Disenhof, a committee member and group director of export compliance and government relations at Cadence Design Systems. Disenhof says that the EDA industry is encountering more overt forms of piracy. "We are taking this seriously, and we think our customers will take it seriously, too," he says.

According to EDAC Piracy Committee member Jim Dou-

WHO ARE YOU BUYING YOUR EDA SOFTWARE



EDA-SOFTWARE
VENDORS ARE TAKING
SOFTWARE PROTECTION
SERIOUSLY, AND YOU
SHOULD, TOO. DON'T
GET HOOKED ON
PIRATED SOFTWARE.

FROM?
x

AT A GLANCE

- ▶ The Business Software Alliance estimates that pirates last year stole \$31 billion worth of software.
- ▶ The most common cause of unintentional piracy in EDA comes from 24/7 worldwide use of a tool that one customer site originally licensed.
- ▶ EDA vendors offer 24/7 licenses, but they are more expensive than site-specific licenses.
- ▶ Users can be held liable for using software that vendors later prove is built on stolen code or trade secrets.
- ▶ Indemnification contracts are only as viable as the companies issuing them.

glas, Reshape's chief executive officer, cases of overt and inadvertent piracy are going on. "A lot of it is simply educating people and speaking with executives about the behavior of their organizations. They may be unaware of what constitutes inadvertent piracy, but, in other cases, they have employees that outright misuse and distribute software their company hasn't paid for," he said, as a member of a recent Design Automation Conference panel.

These problems are worse in countries outside North America and Europe and are especially bad for EDA in China and India. Altium fired its previous distributor in China after discovering that the distributor was selling Altium software on the side, and Altium's chairman claims his company has evidence that the Chinese government uses hundreds of pirated versions of Altium's Protel software for designing military equipment (see sidebar "China presents challenges for EDA"). Altium is pursuing this and related matters with the Australian government, which is currently negotiating a free-trade agreement with China.

WORLDWIDE PIRACY PROBLEM

EDAC and the BSA (Business Software Alliance), a nonprofit software-industry group dedicated to tracking and prosecuting software piracy, educating the public, and lobbying the government on the issue, have no statistics tracking the

impact piracy has had on the EDA industry. But the BSA and industry analysts from research company IDC joined to conduct their first worldwide software-piracy study for the year 2003. And the most recent piracy study concludes that the software industry worldwide sold \$59 billion worth of commercial software in 2004 but that \$90 billion worth was installed, meaning \$31 billion worth of software was pirated.

Although no study on EDA piracy exists, EDA vendors say convincing evidence does exist that EDA-software piracy is on the rise, especially as Asia opens up as a market for design tools. According to the 2004 study, Vietnam, Ukraine, and China top the list. In those three countries, 92, 91, and 90% of all software is stolen, respectively. In India, which has a growing reputation as a strong country in IC and design services, the figure is 74% (Table 1).

Laurie Atkinson, director of marketing at the BSA, says that the 2003 piracy study found that two-thirds of college students participating in the survey said that they have knowingly downloaded unlicensed software from peer-to-peer networks. "They know it is wrong, yet they do it anyway," she says. "And, presumably, they will be taking these attitudes into the workforce. When a company hires a new graduate, unless the company has an aggressive software-management policy in place, that new graduate may be illegally downloading software

and putting that company into jeopardy."

Over the last year, you may have seen greater evidence and received a growing number of e-mail solicitations with URLs likely leading back to China or Russia, in which individuals claim to offer EDA tools at huge discounts. One such e-mail offers users unlimited access to any tool from Magma Design Automation, Mentor Graphics, Cadence Design Systems, or Synopsys for a low fee, and another claims to offer for \$20,000 a workstation with every piece of EDA software from those vendors preloaded. The offer even includes maintenance. The BSA's director of enforcement, Jenny Blank, says that those offers are more likely to be Internet money scams than piracy operations. Still, no shortage of methods to pirate software exists.

TYPES OF SOFTWARE PIRACY

The BSA has identified five major classes of software piracy: end-user piracy, client-server overuse, Internet piracy, hard-disk loading, and software counterfeiting. End-user piracy occurs when a company employee reproduces copies of software without authorization. Client-server overuse occurs when too many employees access a piece of software over a network. Internet piracy takes place when pirate Web sites make software available for free download or in exchange for uploaded programs. It also occurs when Internet auction sites offer counterfeit, out-of-channel, infringing-

TABLE 1 SOFTWARE-PIRACY RATES

20 countries with the highest piracy rates	2004 (%)	2003 (%)	20 countries with the lowest piracy rates	2004 (%)	2003 (%)
Vietnam	92	92	United States	21	22
Ukraine	91	91	New Zealand	23	23
China	90	92	Austria	25	27
Zimbabwe	90	87	Sweden	26	27
Indonesia	87	88	United Kingdom	27	29
Russia	87	87	Denmark	27	26
Nigeria	84	84	Switzerland	28	31
Tunisia	84	82	Japan	28	29
Algeria	83	84	Finland	29	31
Kenya	83	80	Germany	29	30
Paraguay	83	83	Belgium	29	29
Pakistan	82	83	Netherlands	30	33
Bolivia	80	78	Norway	31	32
El Salvador	80	79	Australia	32	31
Nicaragua	80	79	Israel	33	35
Thailand	79	80	United Arab Emirates	34	34
Venezuela	79	72	Canada	36	35
Guatemala	78	77	South Africa	37	36
Dominican Republic	77	76	Ireland	38	41
Lebanon	75	74	Portugal	40	41

Courtesy Business Software Alliance



copyrighted software or when peer-to-peer networks enable unauthorized transfer of copyrighted programs. Hard-disk loading happens when companies load a piece of software onto multiple computer drives. And software counterfeiting occurs when users duplicate and sell exact copies of copyrighted material.

The two most common forms of piracy EDA vendors encounter are inadvertent piracy and intentional “overuser” perpetrators. You may be unaware that you are illegally using software. For example, EDA vendors offer companies a broad range of licensing options that can vary from sale to sale, so users need to be aware of the terms of their licensing agreements. “A majority of companies pirating soft-

ware are actually honest companies, but, for whatever reason, software-asset management is just not at the top of their list of priorities,” says Atkinson. She says that this situation typically occurs in the mid-sized- to small-business sector, which may lack full-time IT personnel to monitor these things.

According to Disenhof, the most worrisome form of piracy for the EDA industry is client-server overuse or, as many in the EDA industry call it, “underlicensing.” “We are seeing one copy, one seat being purchased, then used 24 hours a day, seven days a week on a WAN,” said Disenhof on a DAC panel. “This industry is using the Internet on a global basis today, and, whether they are doing it con-

sciously or unconsciously, having software reside on a server that is accessed around the world may not be licensed legally. Engineers who are picking up the software in China, for example, during the graveyard shift in the United States may not have a legal right to use it. So, we are seeing a general trend of underlicensing across the board.” Disenhof and others point out that most vendors offer terms that grant 24/7 usage of software worldwide, but it is typically much more expensive than a single-seat, perpetual license.

According to Rex Jackson, Synopsys’ general counsel and acting chief financial officer, the other most common form of EDA piracy comes from the intentional overuser. A common profile of an inten-

CHINA PRESENTS CHALLENGES FOR EDA

EDA vendors see China as a potentially huge opportunity for market growth, but most agree that the Chinese government needs to be more diligent about creating and enforcing IP (intellectual-property)-protection laws to ease trade fears.

Altium’s executive vice chairman, Kayvan Oboudiyat, says that Altium has been selling products into China for 12 years and has had an ongoing problem with the practice, as well as with piracy that Chinese consumers, businesses, and even the government perpetrate. “Protel tools are popular in China,” says Oboudiyat. Many employers list Protel on their applications and list it as a qualification for new hires. But the number of qualified users far exceeds the number of licenses Altium has sold there. Part of that problem has been distribution in China. The company has for years sold its software through distributors in China but had to fire its first distributor in China after it

found that the distributor was selling extra copies of Altium software on the side for its own profit.

“Although a majority of them were good, hardworking people, some of them were abusing their position, and, for every one license sold, they were selling a few more on the side,” he says. The company has since taken steps to address that problem by establishing an office in Shanghai and by hiring new resellers. “The only way we can effectively address this issue is by working with resellers and customers and educating them that there is more to EDA products than just the CDs. You can go to any software shop in Shanghai, Beijing, or Shenzhen and buy an illegal version of Protel over the counter. We need to develop a relationship and an emphasis on the value of training.”

The Chinese government has also been ineffective in policing the problem, and Oboudiyat says that, in Altium’s case, it has even been a culprit in some

instances. “There is a lot of goodwill on the part of the Chinese government, but they need to make some radical changes to become effective,” says Oboudiyat. “We know and have solid evidence that some of the largest government-owned military-R&D organizations in China use not just tens but hundreds of illegal licenses. We need to develop relationships with the government and come up with a long-term, sustainable solution.”

Part of the problem may be cultural, vendors and BSA members say. “I don’t know that the Chinese people who do what we think is stealing software actually think they are stealing software,” says Rex Jackson, Synopsys’ general counsel and acting chief financial officer. “I don’t know that they look at it that way.”

To change this situation, all agree education about international law is paramount, but money will ultimately be the factor that makes things change in China. Others point out

that, as Chinese companies start to acquire international companies, adoption of international IP laws will also speed up. Most vendors believe it will just take time. Most point to Taiwan as a prime example, saying that piracy was once rampant, but the problem has decreased as the country plays a larger role in the international business community. “I think it is going to change, perhaps not as fast as we would like, as the Chinese develop their own IP,” says Jackson.

Some large Chinese companies have approached Altium, admitting that they inadvertently own pirated copies of Altium’s software and want a formal, legitimate relationship with the company. “In these cases, we’ve worked with customers to resolve issues and form long-term relationships,” says Oboudiyat. “Over the next five to 10 years, this approach will become a common way to deal with the issue of piracy.”



tional overuser is a customer who acquires just one perpetual license of a flow and then almost immediately drops the maintenance agreement. “We work with our salespeople to identify that profile because it is remarkable how good that match is,” says Jackson. “Once you have identified customers that came in once and then disappeared off the radar screen, you have to ask yourself: Do they still exist, where are they, and how large do you think their design team is?”

Jackson says that all Synopsys contracts give the company the right to audit users to ensure they are not misusing licenses, and Synopsys exercises this right, especially when customers fit the intentional-overuser profile. Synopsys and most EDA companies tend not to pursue every small infringement, simply because doing so is not cost-effective. Synopsys, like many EDA companies, has joined the BSA and is banking on the fact that education on all levels is the key to reducing all forms of piracy over time.

The BSA helps to educate consumers, businesses, and government officials

worldwide about software piracy. Failing that, the BSA also has legal muscle, a Public Action Committee, to push for domestic and international legislation regarding software piracy. It also runs piracy hot lines in most countries.

LEGAL CONSEQUENCES

The BSA’s Blank says that the BSA helps its member companies bring civil suits against offenders, works with criminal-law-enforcement authorities, and operates a high-volume notice-and-takedown program. Both inadvertent and overt software pirates can face criminal charges ranging from fines to jail terms. The FBI doesn’t get involved until the amount of software pirated exceeds \$100,000, a lofty amount for business-software pirating but the price of only one or two tools for pirated IC EDA tools, whose prices average approximately \$40,000 per seat.

Vendors in the United States can seek one of two civil-court remedies if they catch a company or an individual stealing. The first is a \$150,000 fine plus the

cost of the software. According to Blank, vendors take this tack in 99% of piracy cases in the United States. The second remedy is an open-ended civil damage for recovering not only the loss of license, but also a percentage of the revenue pirates generate using end products they developed with the stolen software. Users can also be in legal jeopardy if they use one vendor’s product that is later found to infringe another company’s patent, copyright, or trade secret. “Under the federal Uniform Trade Secret act, customers have full liability if they are using software that infringes a patent or if they purchase software that is stolen,” says Chris Scott Graham, IP (intellectual-property) attorney with Dechert LLP, a law firm that currently represents both Silvaco and Synopsys on their respective IP litigations. California district attorneys can prosecute engineers under Criminal Trade Secret Statute 499C for using a product that violates a trade secret or under the California Penal Code Section 496, which essentially states that receiving any stolen property is a crime.

SILVACO SEEKS LEGAL REMEDY AS SYNOPSIS WATCHES

Users have so far largely ignored the legal wrangling of EDA vendors and continued to use software even if a preponderance of court evidence indicates that the software is tainted. They made this decision largely because they believed EDA vendors had no recourse. They assumed that vendors would not risk losing current or potential customers. Also, they had received indemnification from the vendor from which they had licensed the software.

Silvaco is attempting to debunk this idea and is pursuing former Circuit Semantics customers. In 2003, Silvaco won its misappropriation-of-trade-secrets suit against EDA start-up Circuit Semantics. In that suit, the court ordered Circuit Semantics

to relinquish ownership of its misappropriated source code and other products to Silvaco. According to Chris Scott Graham, Silvaco’s attorney with law firm Dechert LLP, Silvaco is now pursuing its right to recover the cost of the stolen license from those customers as well as a percentage of revenue from any products developed with the stolen software.

For a relatively small company such as Silvaco, the move appears to be a gamble. Silvaco risks burning the bridge that links it to some of the EDA industry’s biggest customers. Silvaco officials won’t comment, but the company’s president and owner, Ivan Pesic, comments extensively at www.deep-chip.com, an EDA-industry-

observing Web site. Vendors have threatened to pursue customers but usually have not done so. Cadence, for example, didn’t pursue Avanti customers after Avanti officials pleaded no contest in criminal court to stealing Cadence code. And Synopsys, which appeared well on its way to winning a trade-secret suit against Nassda before acquiring that company last year, didn’t pursue customers because it ended up inheriting Nassda contracts.

But Synopsys’ Jackson says that the company hasn’t ruled out going after Magma customers, especially those that have continued to license software from Magma even after Synopsys’ legal team presented what appears to be damning evidence in

the form of Magma co-founder Lukas Van Ginneken’s admitting that he used technology developed at Synopsys to design Magma’s products. “Our focus is on winning the Magma case first,” says Jackson. “We’ll see where it goes from there. I am surprised that, in the EDA business, customers figure it won’t be their problem and that someone will work it out so that they don’t have to worry about it. I don’t understand that perspective. I would never say that I’m going to sue everybody that uses Magma tools if we win the Magma case. In the interim, though, given how clear the admissions have been in the Magma case, it surprises me that people would make new commitments to that technology.”



Although EDA vendors commonly sue each other in civil court in patent or trade-secret disputes, EDA vendors have traditionally shied away from suing customers that use infringing software. Silvaco is bucking that trend, and, pending the conclusion of its suit against Magma, Synopsys hasn't ruled out pursuing Magma customers, either (see sidebar "Silvaco seeks legal remedy as Synopsys watches").

HOW TO PREVENT PIRACY

Most EDA tools include security technology such as Macrovision's FlexLM, which essentially functions as a key that allows access to the software for the term of the license. However, the use model for EDA software has been changing and has become more complex. Traditionally, vendors have sold licenses on a per-CPU or per-seat basis, but Suresh Balasubramanian, director of licensing products at Macrovision, says that licensing arrangements are getting more complex because user demands and even the definition of "CPU" are changing. "In the semiconductor industry, we are seeing a trend toward deploying software on mass-computing, where people want to do bigger simulation faster and deploy these jobs on thousands of CPUs," he says. "When you look at new technology trends, where the whole dynamic of computing changes—where you have dual-core CPUs or multithreaded CPUs—publishers are often at a loss as to how to license their software." Macrovision is working with other vendors to do intelligent scheduling to monitor simulation-farm usage. The compa-

ny is also looking at developing programs to prevent pirates from overtly hacking EDA software (see sidebar "How pirates hack EDA software"). "Just as people are determined to break software, one of the things we've put in our software is for crippling pirated software," Balasubramanian says. "So, for example, if someone pirates an EDA tool, their verification won't complete, or their timing will be off, so you frustrate the hell out of them and ensure that they are not productive."

Of course, EDA software doesn't have the greatest reputation for being bug-free. Half-jokingly, vendors agree that EDA lends itself less well to piracy because its software tends to be complex and bug-prone, requiring upgrades and maintenance. Ironically, some vendors say they discovered that they had a piracy problem when an increasing number of non-customers inquired about software patches or sent inquiries to customer support or even formed user groups in countries not allowed to own EDA software. EDA vendors pass the cost of adding greater licensing and security features to their products onto their customers.

HOW TO PROTECT YOURSELF

Due diligence is the key, experts say, to protecting yourself or the company you work for from implication in a software-theft-related lawsuit. Designers and managers need to be aware of the terms of their software-license agreements, and, for example, not access any software that has a geography- or site-specific license. Companies also need to police their employees to ensure that they are not

MORE AT EDN.COM

- + For much more on EDA, visit www.edn.com/eda.
- + And for a list of EDA vendors and organizations related to this article, or to post a comment on this article, go to www.edn.com/050818cs.

bootlegging corporate products for their own personal use or profit. Experts say that your company, as well as the individual employee unknowingly perpetrating the crime, can incur huge fines. According to the BSA, the most common way that companies discover piracy is after a disgruntled employee reports it. If your company is using software that is stolen and such an employee reports it, the piracy can damage your company, division, or group to the point that you may find yourself out of a job.

If you are licensing software from a vendor that is later sued or is currently being sued by another vendor for patent or copyright infringement or misappropriation of trade secrets, that other party can also sue you if doing so ultimately wins the legal dispute. Because of this risk, experts say that customers have every right to demand to see all pertinent evidence in the case to assess whether the vendor can win the case or is healthy enough to honor indemnification if it loses the suit.

"Indemnification is a contractual agreement that says, 'If I'm found to have stolen someone's product, I will replace what I sold you with a noninfringing copy, or I will refund your money or defend you from a third party claiming you have done something wrong,'" says Graham. "In most cases, indemnifications are not worth the paper they are written on." Graham notes that insurance companies do not back indemnification contracts, and, therefore, any indemnification contract is only as strong as the size, health, and cash balance of the company offering it. **EDN**

HOW PIRATES HACK EDA SOFTWARE

Suresh Balasubramanian, director of licensing products at Macrovision, says that Macrovision-licensing software developers are in a cat-and-mouse game with hackers. Balasubramanian says that people have illegally hacked into EDA software in three ways. The first way is by configuring multiple workstations or computers to appear to the license as just one computer. Vendors roughly three years ago defeated this approach. Once defeated, hackers then started illegally gener-

ating license keys to perpetually access software. Advanced encryption technology from Cirticom a couple of years ago defeated that approach. Hackers now have to enter the binary code and hack the licensing code. Balasubramanian says that a version of FlexLM, slated for release this year, will allow users to distribute that code throughout their program and tie it closely to functions, so if someone hacks a code, the tool will run but give inaccurate results.

You can reach Senior Editor Michael Santarini at 1-408-345-4424 and michaelsantarini@reedbusiness.com.

