Ethical Hacking and Countermeasures
Version 6

Module L

Software Piracy and Warez

CEH

Certified Ethical Hacker

In Business Today

Reducing software piracy by 10% would increase IT spending to R6 billion

28 January 2008
BSA

Reducing software piracy over the next four years in South Africa could create a stronger local information technology (IT) sector, generate new high paying jobs and contribute to the country's economy, according to a new study released today by the Business Software Alliance (BSA).

The study, commissioned by BSA and conducted independently by International Data Corporation (IDC), notes that the IT industry already is a major contributor to jobs, tax revenues and South Africa's gross domestic product (GDP). The South African IT industry is projected to deliver 99 000 jobs, R84 billion in economic growth and over R30 billion in tax revenues by 2011.

Reducing South Africa's 35% software piracy rate by 10 percentage points would have a "multiplier effect" and increase those economic benefits, generating 1200 additional jobs, R480 million in tax revenues and R6 billion in spending in the local IT sector over the next four years.

"When countries take steps to reduce software piracy, everyone stands to benefit," said Alastair de Wet, chairperson of the BSA in South Africa. "With more and better job opportunities, a stronger, more secure business environment and greater economic contributions from the already robust IT sector; reducing software piracy delivers tangible benefits for governments and local economies."

IDC finds that for every R1 spent on legitimate packaged software, an additional R1.25 is spent on related services such as installing the software, training personnel, and providing maintenance services. Most of these benefits accrue to locally-based software services and channel firms – meaning the greatest proportion of the economic benefits from lowering software piracy stay within the country.

Source: *http://www.moneyweb.co.za/*

Microsoft Helps Nab $900M Piracy Ring

Feb 8, 2008

SEATTLE (AP) — Microsoft is telling the tale of a major software piracy investigation that weaved through 22 countries, hoping would-be pirates will think twice if they know how far the company will go to protect its computer code worth billions in revenue each quarter.

Near-perfect knockoffs of 21 different Microsoft programs began surfacing around the world just over a decade ago. Soon, PCs in more than a dozen countries were running illegal copies of Windows and Office, turning unwitting consumers into criminals and, Microsoft says, exposing them to increased risk of malicious viruses and spyware.

The case began to turn in 2001 when U.S. Customs officers seized a shipping container in Los Angeles filled with $100 million in fake software, including 31,000 copies of the Windows operating system.

From there, Microsoft pushed the investigation through 22 countries. Local law enforcement officials seized software, equipment and records, and made arrests. A court in Taiwan handed down the last of the major sentences in December. Microsoft estimates the retail value of the software the operation generated at $900 million.

"That is a tremendous accomplishment," said James Spertus, a former federal prosecutor in Los Angeles who later led anti-piracy efforts for the Motion Picture Association of America. "There are only going to be a few cases like this a decade."

Now Microsoft is eager to talk about the experience because taking down that operation — responsible for about 90 percent of the fake software the company found between 1999 and 2004, more than 470,000 disks — didn't actually stop piracy. It just left room for more counterfeiters to rise. Microsoft hopes would-be pirates will think twice if they know how far it will go to protect the computer code worth billions in revenue each quarter.

The pirates mimicked complex holograms stamped directly onto disks and packaging materials embedded with the kind of tiny safety threads used in making money. In some cases, it took experts with microscopes to notice that disks printed with codes used by legitimate software factories lacked certain minuscule, unique smudges.
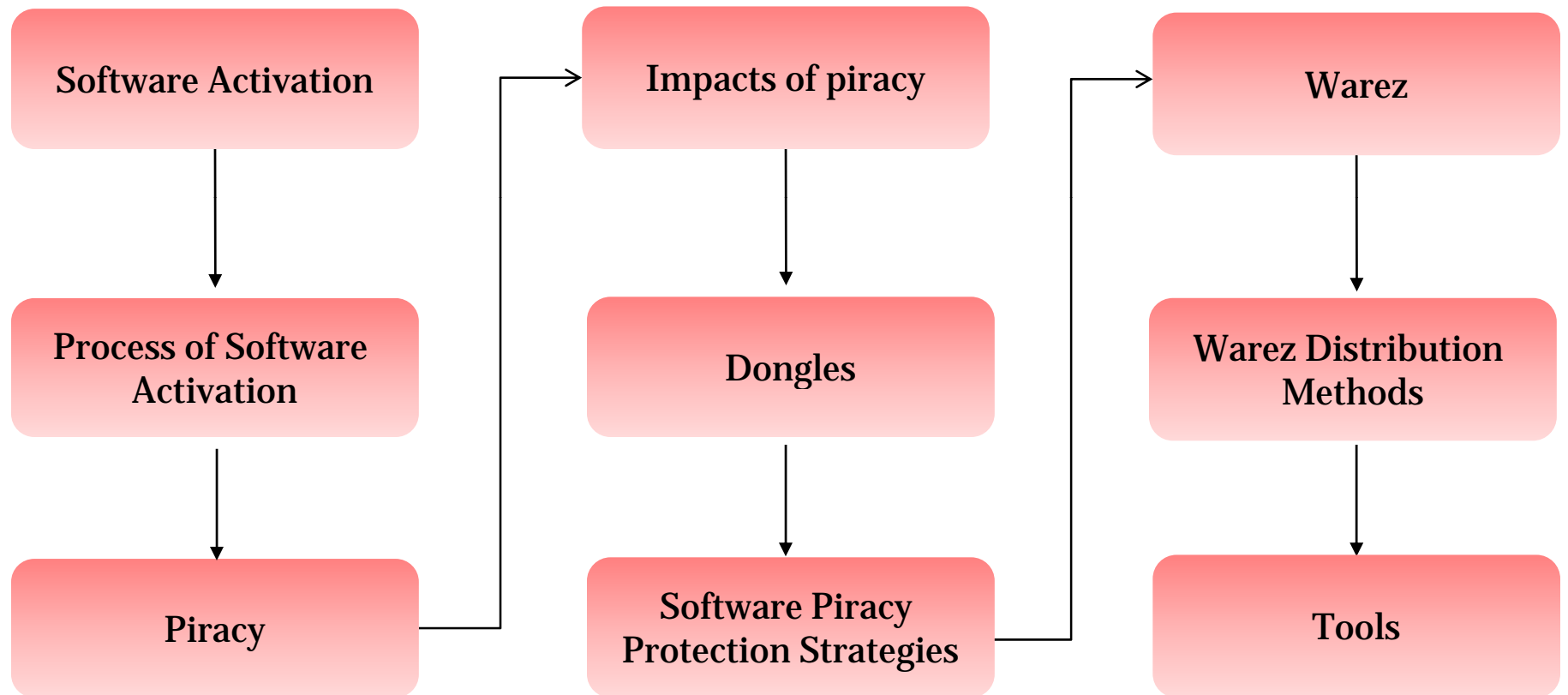
Source: *http://ap.google.com/article/*

This module will familiarize you with:

- Software Activation
- Process of Software Activation
- Piracy
- Impacts of piracy
- Dongles
- Software Piracy Protection Strategies
- Warez
- Warez Distribution Methods
- Tools

CEH Certified Ethical Hacker

Software Activation

Impacts of piracy

Warez

Process of Software Activation

Dongles

Warez Distribution Methods

Piracy

Software Piracy Protection Strategies

Tools

Software Activation

EC-Council

Software activation is the process of obtaining a license for software so that it becomes active and ready to be used on the computer

This can be done automatically over the Internet or manually by phone, fax, or email

Only that software can be activated for which the license has already been purchased

Computer Requesting Activation — Internet Connection via Encrypted HTTPS Transfer — Square One Licence Activation Server

1 • the software vendors register with the Software Activation Service (SAS)

2 • After activation of the account of the software, the vendor can operate the account and generate Product Keys for their products using the SAS website

3 • These Product Keys are then integrated with the vendor's software

4 • Each copy of the software is labeled with the Product Key and sold to the end-users

EC-Council

Request Product Key

Issue Product Key

Vendor

Software Activation Service

Step 1 — Integrate with Activation Service

Step 2 — Build License and Issue product key

Step 3 — Label software with product key for release

Product with Key
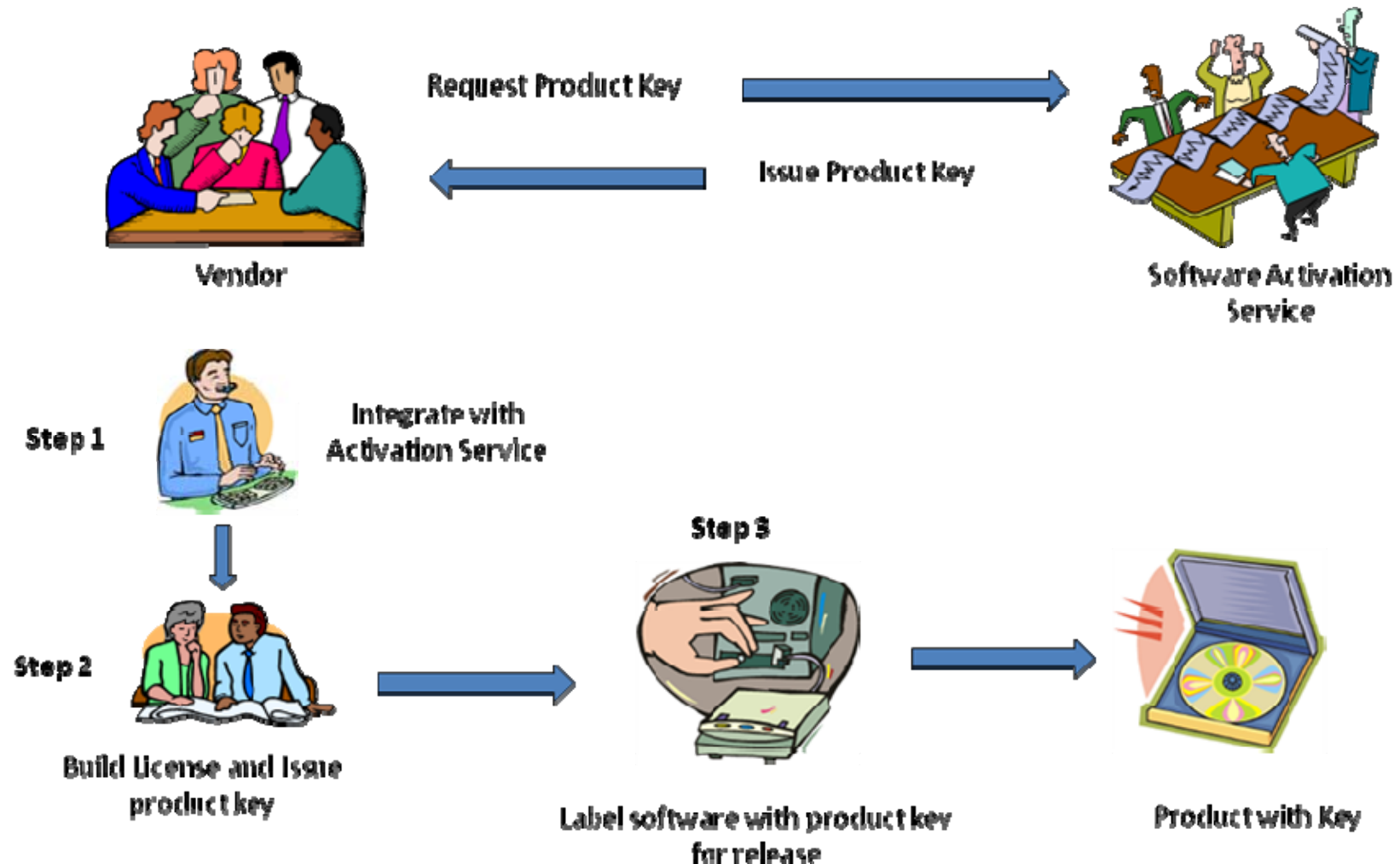
Process of Software Activation (cont'd)

5
- The end-user buys or downloads the product from the vendor and installs it on a computer

6
- During installation, an Authentication Number consisting of the unique Computer ID and time stamp is sent from the end-user's computer along with the Product Key to the Software Activation Service

7
- Product Key and Authentication Number are validated and a License Key is sent to the end-user's computer

8
- Now the end-user can start using the software

Piracy

EC-Council
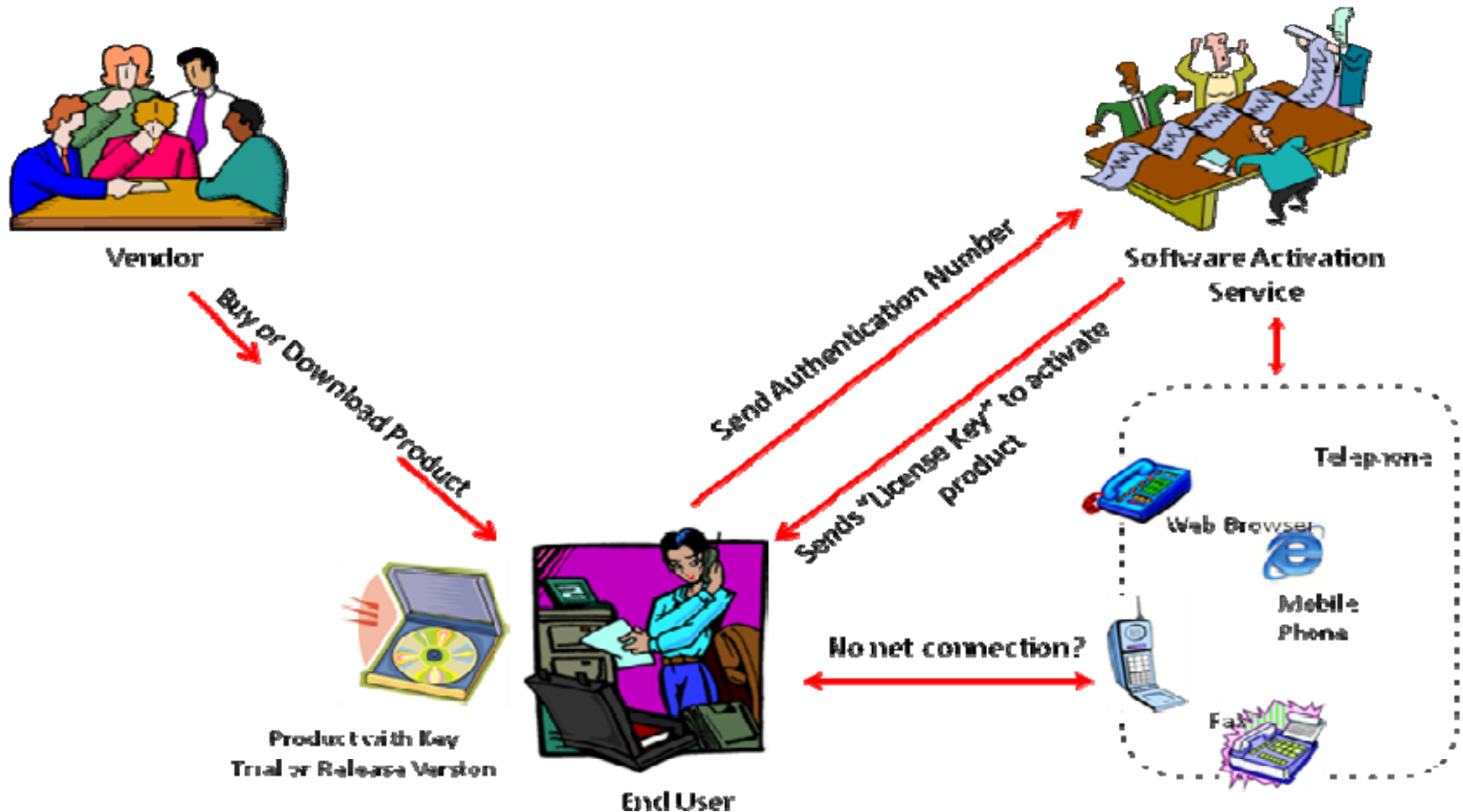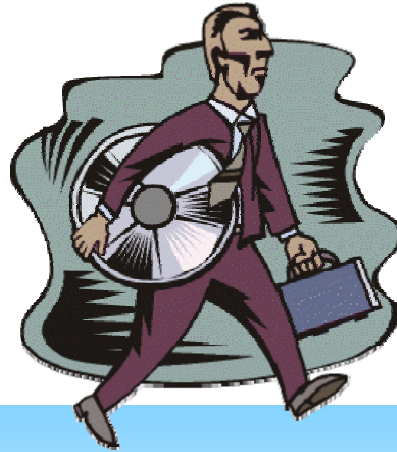
41 firms in software piracy probe

By Jane Bradley

A CRACKDOWN on software fraud in Glasgow has resulted in 41 companies being placed under investigation by the Business Software Alliance (BSA).

The figure is a near-20-fold increase on the same period the previous year.

The clampdown was launched in Scotland's biggest city in November after the organisation revealed Glasgow was the third-worst city in Britain for software piracy, after London and Manchester.

The BSA wrote to about 8,000 small-business owners, warning them to ensure their software was legal. If businesses were found to be breaking the rules, but agreed to comply within 30 days, the organisation agreed not to take any legal action. The 41 businesses reported for alleged piracy – which span many sectors, from engineering and media to architecture – will now be scrutinised and face potential legal action.

Companies found to have intentionally flouted the rules and continue to use counterfeit software could be liable for fines of thousands of pounds.

Julie Strawson, UK committee chair of the BSA, said: "Those businesses that have ignored warnings will now face the consequences of failing to take this issue seriously."

Source: *http://business.scotsman.com/*

Software piracy is the illegal distribution and/or reproduction of a product for business or personal use

Each of the following activity is a form of software piracy:

- An individual copying software for a friend
- A business under-reporting the number of computers using the software
- Sending your username and password to friends
- Downloading cracks or key generators to by-pass security features

EC-Council

CEH Certified | Ethical | Hacker ™

Internet piracy is the uploading of commercial software on to the Internet for anyone to copy commercial software from any of the services

It includes making available the pirated software over the Internet and offering it for sale

Internet piracy is the most rapidly expanding type of piracy and the most difficult form to combat

Internet piracy can take many forms:

- Auction Site Piracy
  - This type of piracy occurs when seller burns software on to CD-ROMs, and offers it for online selling
- Bulletin Board Services & News group piracy
- FTP Sites
  - In this, FTP allows the pirates to download or upload the files to the site

Auction Site Piracy

Sample of FTP pirates

Source: *http://www.siia.net/*

EC-Council

Warez

- A website that allows users to download commercial/legitimate software for free of charge

Source: *http://www.siia.net/*

EC-Council
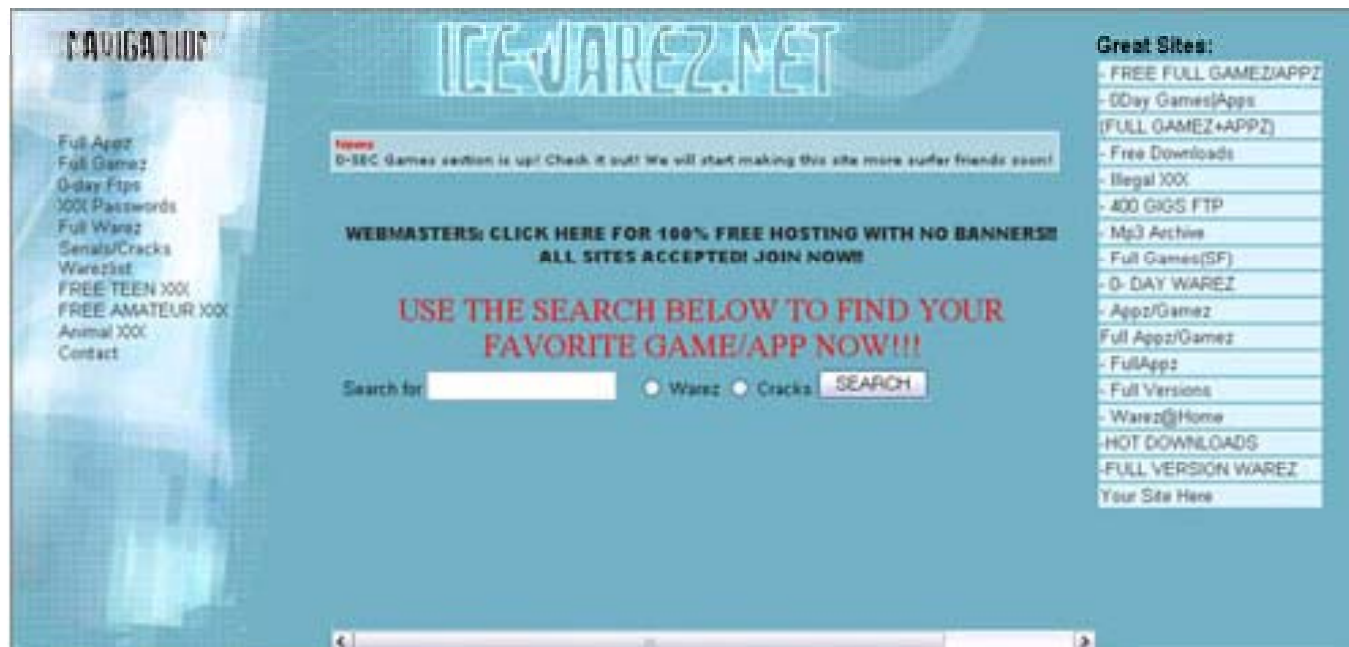
Peer-to-Peer

- Due to the distributed and anonymous nature of P2P sites, these are used for distribution of unauthorized software and content

Cracks/Serial Numbers sites

- Cracks are small files that circumvent copyright protection and the key generator is an application that uses the serial number or CD key-generating algorithm to create fake

Internet Relay Chat

Site provides crack and serial number services

EC-Council

Abusive Copies occur when a single legitimately acquired CD or downloaded version of a software program is used to install the software on multiple PC's

The original copy of the software is licensed to be installed only on a single machine or to be used by no more than one person at a time

A large percentage of abusive copies are made by users who would purchase licensed copies if they do not have an option of making an abusive copy

Installation of an abusive copy is convenient rather than lack of motivation or resources to purchase

Pirated copies are unlicensed physical copies of an original program CD that are manufactured and sold by an illicit manufacturing and distribution operation

They are misrepresented to the end-user as legitimate versions of the program and sold at close to full price

They are also grouped with several other programs on a CD in a clearly pirated and typically steeply discounted bundle

Fake pirated copies are a major income loss for software companies since purchases at close to full retail price that would otherwise be routed through the legitimate distribution system are being lost

These are the original copies of the software that are modified by crackers to prevent any copyright protection mechanism that may have been implemented in the program

The modification is performed by disassembling the executable program and searching for copyrighted segments

Those segments are then directly modified to disable them

Cracked versions of programs are distributed in an underground fashion on the Internet

Impacts of Piracy

Local software companies have lost their income by competition with pirated software from abroad

Government lost tax revenues

Most of the employees lost their jobs due to lack of a legitimate market

By using Internet and Peer-to-Peer (P2P) networks piracy rates has been increased

Over 60% of Internet traffic is driven by P2P downloading which clearly shows the level of piracy on Internet

Software Piracy Rate in 2006

CEH TM — Certified Ethical Hacker

Software piracy rate in selected countries—2006
Percent

Country	Percent
Indonesia	85
China	82
Russia	80
Thailand	80
India	71
Italy	51
Spain	46
Czech Rep.	39
Canada	34
USA	21
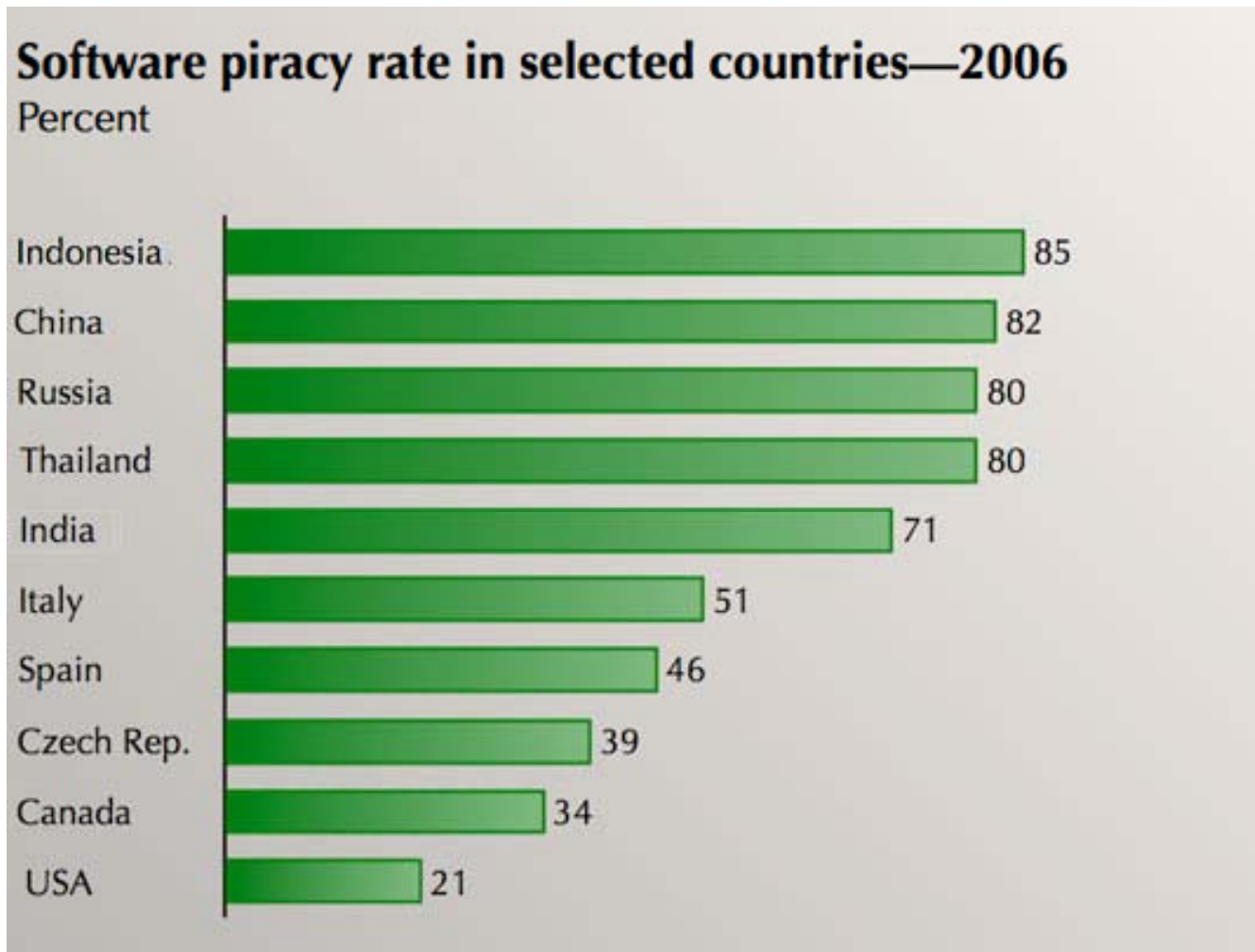
Software Piracy rates in the year 2006

Source: *http://arstechnica.com*

Piracy is not neutral like other infrastructural modes but mediates the media that work under its command of reproduction

piracy requires particular conditions for recording, transmitting and retrieving data

Constant copying wears down data storage, degrading image and sound, disturbing the signal of media content with the noise produced by the means of reproduction

Dealers involve s in pirated media by reproduction of original copy and recording data on cheap tapes by the use of poor quality machines

Software Copy Protection Backgrounders

EFCC Moves to Halt Software Piracy

By James Emejo, 02.20.2008

Worried by the rising cases of Intellectual Property (IP) theft in the country, the Economic and Financial Crime Commission (EFCC) has arrested some computer vendors operating at the popular computer village in Ikeja.

The clampdown is expected to discourage further sale and use of pirated computer software.

Mr. John Obora, Secretary, Computer and Allied Products Dealers Association of Nigeria (CAPDAN), the umbrella body of the vendors in the market told THISDAY five of its members were invited by the commission in line with a petition written against some vendors by software giant, Microsoft for using pirated operating systems.

Although the association has expressed its readiness to cooperate with Microsoft in curbing the sale of pirated software in the market, it however frowns at the use of the EFFC to address the problem.

He recalled that CAPDAN and Nigeria Copyright Commission have severally carried out raid on sellers of pirated software at the market where pirated software were seized and destroyed.

He warned that the act of intimidation being adopted by Microsoft is bound to flaw the exercise.

He noted that the association had already reached an agreement with Microsoft the vice president when he visited the market in November last year, when it was agreed that the sellers should be trained in other means of livelihood as part of a rehabilitation initiative.

Obora however, urged Microsoft to consider reducing the cost of its software as a way of discouraging piracy.

ICT is believed to provide more than 10 million direct jobs and contributes approximately $1 trillion dollars to the global economy. But theft of IP deprives Nigerian professionals of the revenue they have rightly-earned and the government of the taxes that can be derived from that revenue. The local music industry has 40 percent of its products copied, and sold illegally.

Source: *http://www.thisdayonline.com/*

CD Key Numbers

CD key is a software activation number that allow user to install software on the PC

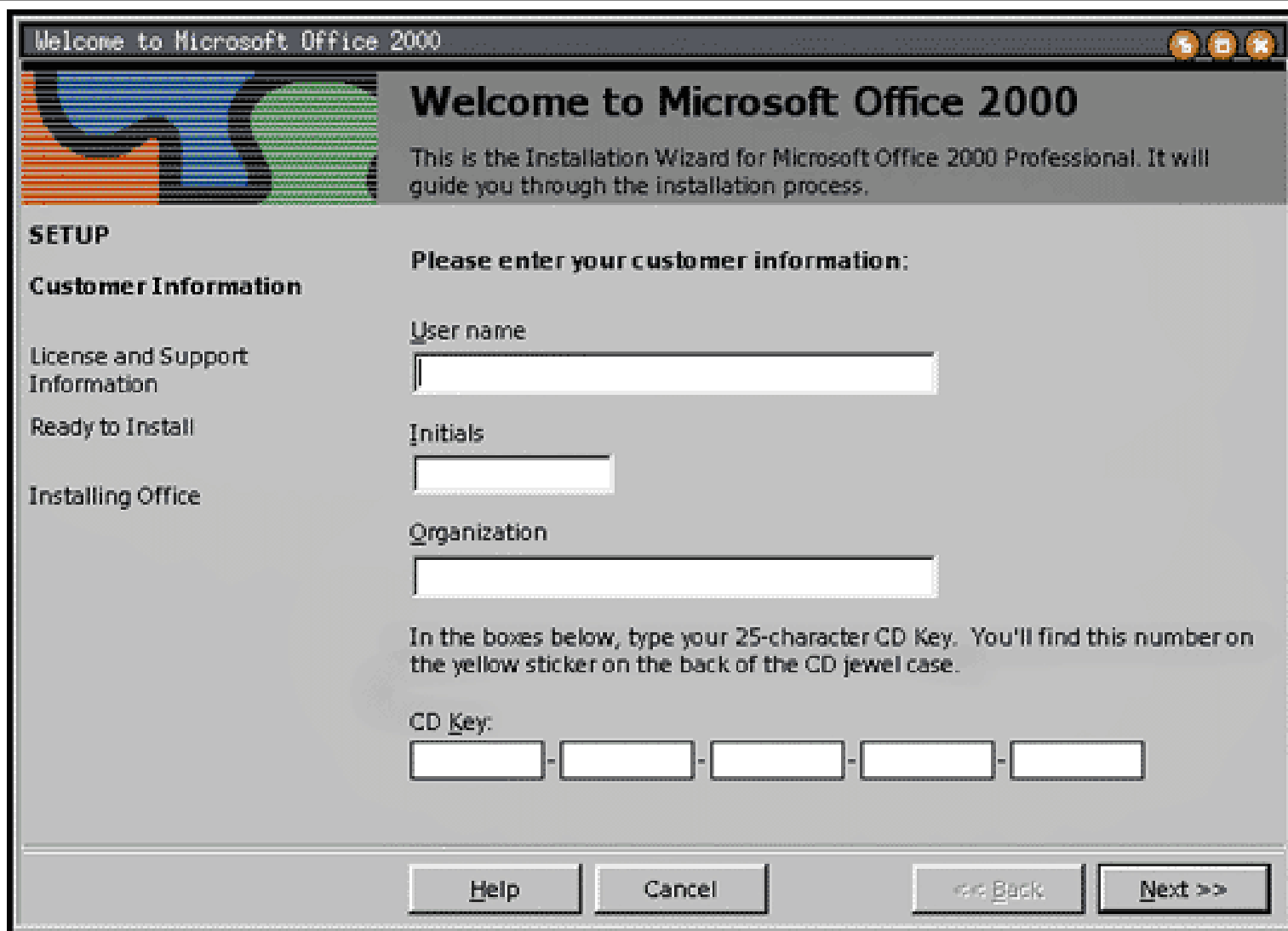It is supplied by the software vendor with the CD as a label attached to the case

User must enter the CD key during the installation of software

The CD key number entered by the user must match the pattern stored the on CD

Sometime this CD key is different for each user or sometime it is only different for the different production runs of the software
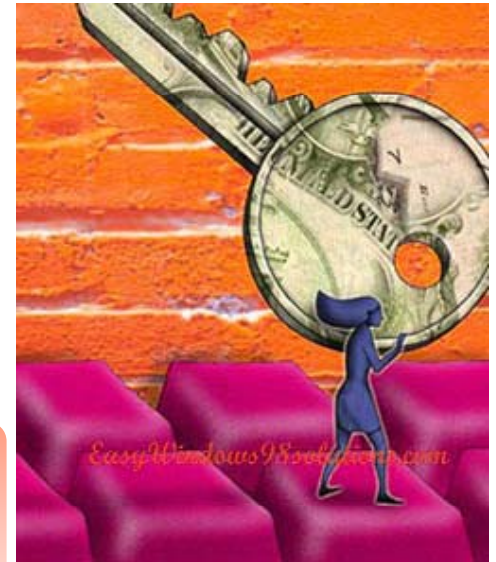
CEH ™
Certified | Ethical | Hacker

This is a copy protection mechanism used by some application

It is hardware device used to connect printer port, USB port or serial port on a PC

It checks to see that the correct dongle in place when protected media starts

These are more difficult to install and use because they require special hardware driver

They can work with the use of printer and scanner

CEH
Certified | Ethical | Hacker ™
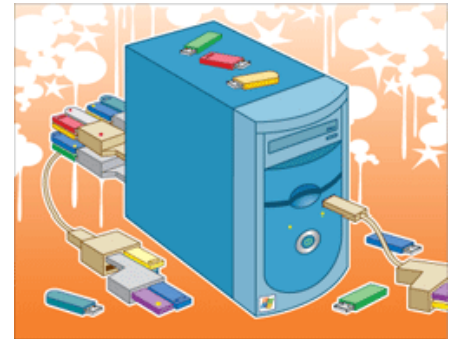
Media Limited Installations is a copy protection mechanism used by software applications

It referred to as the Media Limited method, because it requires the program can be installed from a re-writable media such as a floppy disc

The installation program counts each installation to an install counter on the re-writable media

When the specified installation counter is exceed then no additional installation will be allowed

It requires a floppy disc that cannot be copied by normal accessible disk copying methods.

EC-Council

It is a copy protection mechanism used by some software applications

This mechanism requires the computer must contain a CD-ROM to allow software operations

When program is start, this method will check for the presence of the CD every certain number of times

This mechanism need the installation media must be manufactured in a manner that cannot be copied by normal accessible disk copying methods

Hidden Serial Numbers

It is a copy protection mechanism that creates a pseudo-random serial number after installation and hides the number on the PC

The serial number is hidden in either an encrypted file or in a special system file location like the registry

The user must complete registration process to allow full operation of the program

During the registration, the user sends the serial number into the application vendor, who verifies that this user is a legitimate

The application vendor then sends the customer with the correct password for that serial number

When the application starts, it reads the value of the serial number and checks that the password entered by the user for that serial number is correct or not

Serial Numbers		
	Total: 100 Users	
Serial # 987	100 Users	7/15/99

C|EH Certified Ethical Hacker
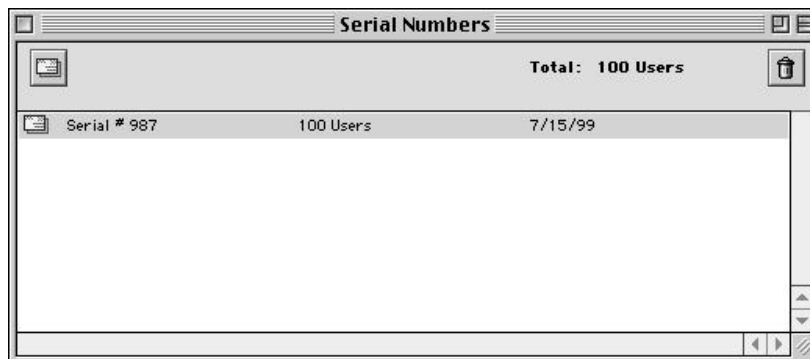
DRM restricts the use of digital files in order to protect the interests of copyright holders

DRM technologies can control file access, altering, sharing, copying, printing, and saving

DRM technology may be contained within the operating system, program software, or in the actual hardware of a device

Some DRM technologies have been developed with little scope for privacy protection

DRM systems can prevent the anonymous consumption of content

The copy protection system tries to prevent illicit copies from being made from either the analog or digital I/O channels of DVD recorders

The DVD copy protection system is designed to support a copy generation management system

This requires at least two bits of information to be associated with a piece of video indicating one of the following copy states:

- Copy_never
- Copy_once
- Copy_no_more
- Copy_freely

Warez

Trade Group Names Top 10 Pirated Software

Software titles most pirated by companies last year include Symantec Norton AntiVirus, Adobe Acrobat, Autodesk AutoCAD, Roxio Easy CD/DVD Creator, and others.

By K.C. Jones
InformationWeek
February 22, 2008 03:50 PM

The Software & Information Industry Association said it hit several milestones in its fight to preserve copyright protections last year.

The SIIA released its Anti-Piracy Year in Review this week, noting that it reached its largest piracy settlement with an auction site and its first settlement through its Corporate Content Anti-Piracy Program.

The trade association for the software and digital content industry said it received 427 reports claiming corporate end-user piracy and 17% of the tips were "judged sufficiently reliable to pursue." The SIIA said that most of the pirated software consisted of productivity tools, including word processing, office suites, report design, and Web design.

In the report, SIIA touted its corporate software piracy case against Florida Benchmark, which cooperated with SIIA, conducted an audit, found it used unlicensed software, and settled with SIIA for $150,000. And, under its Auction Litigation Program, SIIA scored a $250,000 settlement for Symantec (NSDQ: SYMC) software in Symantec, et al. v. Chan, et al.

Also last year, SIIA expanded public education and outreach through new campaigns like: "Don't Get Mad, Get Even," which encourages consumers duped into buying counterfeit software to provide tips in exchange for cash. The industry group also published three new Software Buyer's Guides on how to spot and avoid illegal software on auction sites.

Under its Corporate Content Anti-Piracy Program, SIIA settled its first case while advocating for the Associated Press, Dow Jones & Co., Nielsen, Reed Elsevier, and United Press International.

Source:
http://www.informationweek.com/news/

Warez is used by software "pirates" to describe software that has been stripped of its copy-protection and made available on the Internet for downloading

The most popular downloads at warez sites include applications from major vendors such as Microsoft, Symantec, Macromedia, and Adobe Systems

CEH ™
Certified | Ethical | Hacker

Apps / Appz

Cracks / Crackz

Games / Gamez

Moviez

NoCD/NoDVD/FixedExe

TV-Rips

Mp3

E-Bookz/ebooks/e-books

Scriptz

Templates

DOX

0-Day Warez

MVids

Warez is distributed by the cracker or cracking crew, it is then compiled and split into .rar or .zip files for compression

An ".nfo or file_id.diz" is created to promote who created the release

The release is moved to the of couriers group, then they will upload it to private FTP server known as Topsites

Release then downloaded by the users of FTP server and spread to IRC channels, sharing sites and to p2p protocols such as BitTorren

From there the release can be downloaded by millions of users all over the world

Mail

Modem

File Transfer Protocol (FTP) and File eXchange Protocol (FXP)

Xabi Direct Client Connection

Hypertext Transfer Protocol (HTTP)

Peer-to-peer (P2P) clients such as eMule (ED2K) Limewire, Warez P2P (iP2P), and BitTorrent (BT)

Tools

EC-Council

CrypKey is a leading global provider of software copy protection and license management solutions

CrypKey products are PC-compatible, including Windows 98, Windows NT, Windows 2000, Windows 2003, Windows ME, and Windows XP

CrypKey protection intelligently manages network licensing on Microsoft networks

CrypKey protection is fully compatible with all installer systems on the market

EnTrial Tool

The EnTrial Administrator is used to create a unique Generated Code and Unlock Key for each product/package installation

Personal ID:

- It is unique for each computer
- It is a combination of both hardware and software that compose the installation computer

Generated Code:

- The Generated Code is "baseline" from which the "Unlock Key" is created

Unlock Key:

- Unlock Key is created using the Personal ID and the Generated Code

EnTrial - Software Product Registrations Administrator

File   Help

Key Generation | Distribution Files

Product Key Generation

Product & Packages - Step 1

Product: My Application

Package: Basic Application

Code Generated at time of Registration - Step 2

Generated Code: 2926S112556221-520b158k-6c57h164-3955IB4852132336

Product Name: My Application

Product Code: e851b025

Package ID: 461f75a6

> 2. Email/relay Generated Code & Unlock Key

[Create Generated Code]

Unlock Key Generated from Personal ID (Computer) - Step 3

Unlock Key: 410149a31140

Personal ID: 170393861-3696609157

> 1. User Supplies Personal ID

[Create Unlock Key]

[Done]

Product Registered. Thank you!

The target application will display the Activation/Registration dialog below

Register My Application

Enter Your Registration Code:

2926S112556221-520b158k-6c57h164-3955IB4852132336

Enter Your Unlock Key:

410149a31140

Your Personal ID:

170393861-3696609157
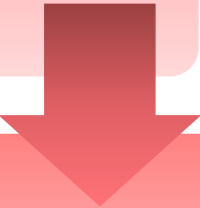
My Application Basic Application

Instructions

Say anything here such as, IMPORTANT: reply to your order email with your Personal Code from the My Application Dialog.

Phone: 515-555-5555

Fax: 515-555-5554

E-mail: support@mycompany.com

[Purchase License]   [**Proceed**]   [Cancel]

Along with the required EnTrial binaries, a EnTrial Distribution file is required in each software distribution created

After creating the basic package, information in the Distribution File Creation GUI can be filled out

Create the Distribution (trr) File by clicking the "Save As Application Reference File"

EnTrial - Software Product Registrations Administrator

File   Help

Key Generation   **Distribution Files**

Distribution File Creation

Application Reference Information

Products: My Application

Product GUID: 28b84f0f-322b-4281-af7f-9b75ca943f74

Product Id: 296f4fff

Version: 1.0

Packages: #   Basic Application (296e5340)

Number of Trial Days: ● 30___

Expiration Date: ○ 7/21/2007

Number of Runs: ○

○ Demo

Order Information

Phone: 515-555-5555   Fax: 515-555-5554

eMail: support@mycompany.com

Online Order URL: www.mycompany.com

Order Instructions:

✱ Say anything here such as, IMPORTANT: reply to your order email with your Personal Code from the My Application Activation Dialog.

Load Default   Save As Default

Application Reference (.trr) File

Open Application Reference File

Save As Application Reference File

Done

Register My Application

Enter Your Registration Code:

Enter Your Unlock Key:

Your Personal ID:

170393861-3696609157

My Application Basic Application

Instructions

✱ Say anything here such as, IMPORTANT: reply to your order email with your Personal Code from the My Application Activation Dialog.

Phone: 515-555-5555

Fax: 515-555-5554

E-mail: support@mycompany.com

Purchase License   Proceed   Cancel

The target application will display the above Activation/Registration dialog

---

The next time the "My Application" product is selected, the above Order Information will be displayed.

Load the saved Default text "over" the currently displayed Order Information.

EnTrial Tool: Distribution File

EnTrial SDK will record the date and time that the software runs for the first time

The SDK will return the remaining number of trial days to the software

SDK will return the following:

- Expiration Date
- Number of Trials
- Demo

Number of Trial Days: ⊙	_____
Expiration Date: ○	7/21/2007 ⌄
Number of Runs: ○	
○ Demo	

Products and Package information that is entered in the Initialization Dialog:

Product Name:
- For a consistent user experience, each product should be named according to the name of the software application

Product ID:
- The Product ID should be an alpha-numeric string

Licensing:
- EnTrial is licensed per product

Package Name:
- Packages can be named as to their functionality such as "20 user Add-On"

Package Code:
- The Package Code should be an alpha-numeric string

Product & Package Initialization

Welcome to EnTrial Software Activate System.

Please fill out the Product (Application) and primary Package information.

Product & Package

Product Name (not changeable once set)

Product ID (not changeable once set)

04ba3241

GUID

d9c7932d-aea5-4a17-a459-e475ed463053

Bacic Package Name:

Basic Application

Basic Package Code:

d5a389db

OK   Cancel

Click the Packages link on the Distribution Files Tab to bring up the Add Package GUI

C|EH ™
Certified | Ethical | Hacker

This is a software toolkit that allow any developer to protect its developed software against piracy and illegal copies in one single row of code

Tool: Crack Killer

Crack Killer is a database application that enables software authors to track and report web sites hosting cracks, serials, and pirated versions of their software

It uses a solid database engine that keeps track of active and inactive pirate software sites

Software vendors can use this software to track sites that contain links to pirated versions of their software

After entering the sites and e-mail contacts for these sites, they can send a tailored complaint notice

DMCA complaint notices can also be sent

Crack Killer: Screenshot

Logic Protect is a reliable anti-piracy, copy protection, software activation, and license management system

It provides high level of security and protection against illegal software copying and distribution

It offers unprecedented level of protection for applications that require access to Internet

It supports all kinds of software activation (including Phone Activation and Software-as-a-Service (SaaS) features)

EC-Council

Logic Protect

6.0

Products | Users | Violations | Messages | Settings | Log Off

Add New Product | Refresh

Product Name (click on Product Name to edit) ▲	Version	Refresh Rate (minutes)	Description	SaaS	Modules	Auto Messages
Product 1	1.0	2	Description goes here - (not saas, has no modules)			
Product 2	2.1	5	Description goes here - (saas, has modules)	Yes	✏	Edit
Product 3	1.4	10	Description goes here - (not saas, has modules)		✏	
Product 4	5.0	3	Description goes here - (saas, has no modules)	Yes		Edit

Page 1 from 1 Display [20 ▾] records on page 1

Add New Product | Refresh

Copyright © 2006 Logic Software Inc.

Software License Manager is used to store important information about your applications

It provides security for information such as:
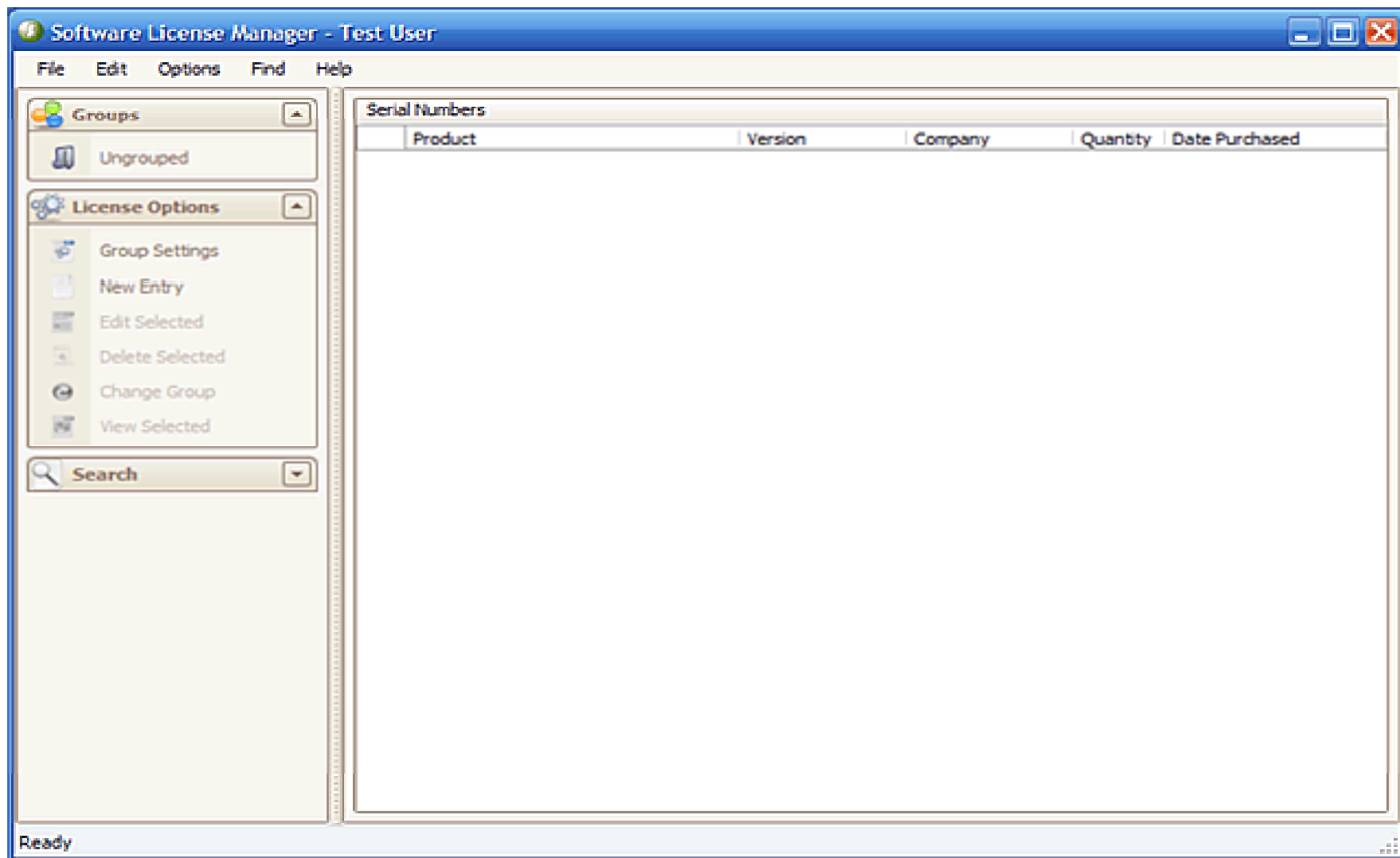
Serial numbers

Software information

Vendor information

License information

Billing information

Software License Manager: Screenshot

CEH
Certified | Ethical | Hacker

Quick License Manager creates professional and secure license keys to protect your software against piracy

It creates permanent or evaluation (trial) license keys in a snap

It can create generic keys that are not bound to a PC or computer-bound license keys

With Quick License Manager, you can add licensing to your software application in less than 1 hour

Tool: WTM CD Protect

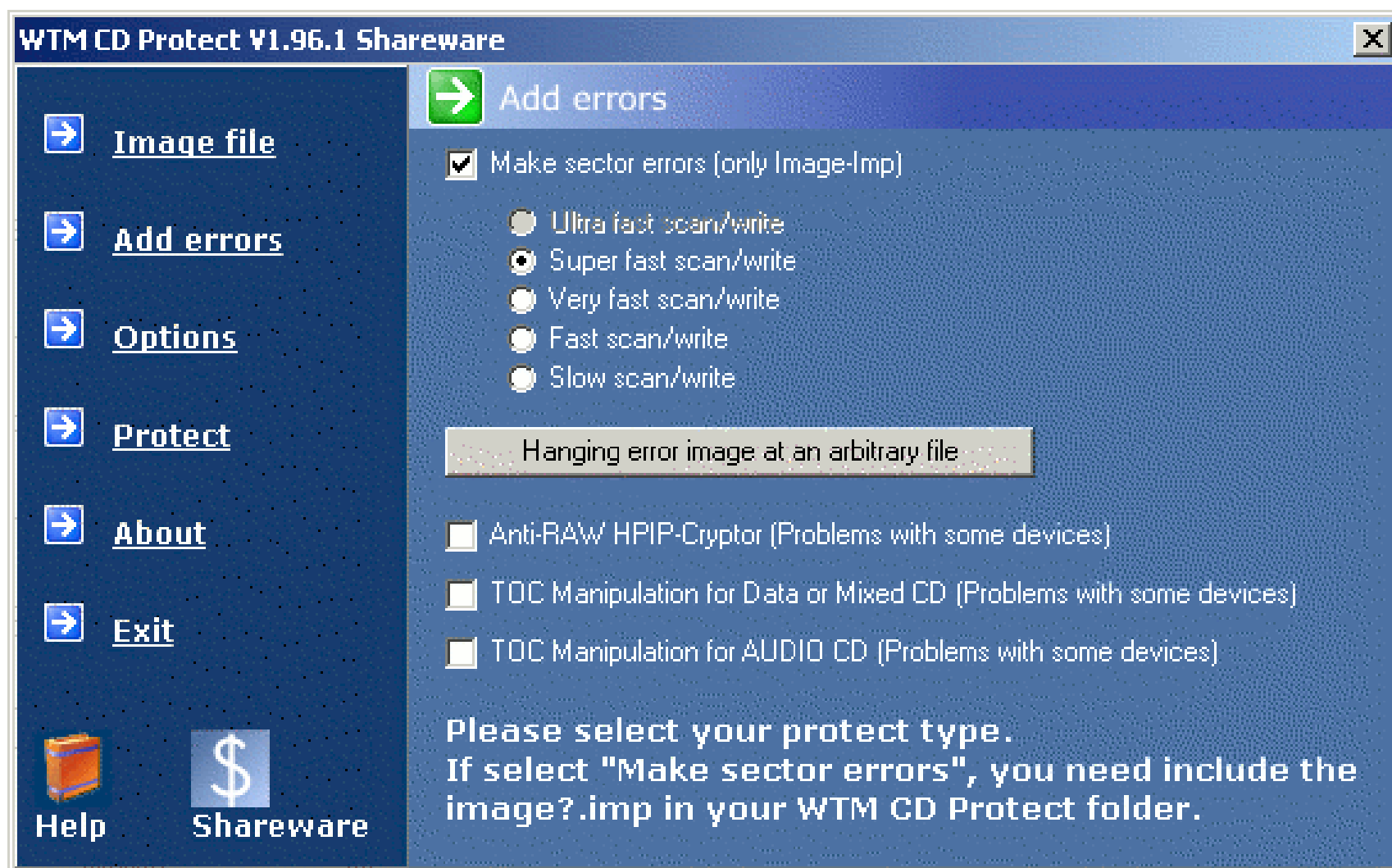WTM CD Protect - Protect your CD against illegal copy

It provides more profit with less illegal copies

It is used to create your own copy protection for your music, video, or data cds

This copy protection system is easy to use and has a strong protection

WTM CD Protect: Screenshot

WTM CD Protect V1.96.1 Shareware   [×]

→ **Add errors**

→ Image file

→ Add errors

→ Options

→ Protect

→ About

→ Exit

Help   Shareware

☑ Make sector errors (only Image-Imp)

○ Ultra fast scan/write
● Super fast scan/write
○ Very fast scan/write
○ Fast scan/write
○ Slow scan/write

[Hanging error image at an arbitrary file]

☐ Anti-RAW HPIP-Cryptor (Problems with some devices)

☐ TOC Manipulation for Data or Mixed CD (Problems with some devices)

☐ TOC Manipulation for AUDIO CD (Problems with some devices)

Please select your protect type.
If select "Make sector errors", you need include the
image?.imp in your WTM CD Protect folder.

Summary

Software activation is the process of obtaining a license for software so that it becomes active and ready to be used on the computer

Software piracy is the illegal distribution and/or reproduction of a product for business or personal use

Some software applications use a copy protection mechanism which is referred by end-users as a Dongle

Warez is used by software "pirates" to describe software that has been stripped of its copy-protection and made available on the Internet for downloading

"What Color Is The Parachute You Used To Move Your Cheese While Winning Friends And Influencing People In India? With a title like that, my book can't miss!"

Copyright 2002 by Randy Glasbergen.   www.glasbergen.com

"I've had to reprogram my voice recognition software six times — I hate puberty!"

GLASBERGEN