ANTI-PIRACY LOCK

SYNOPSIS

Introduction :

The software industry is the backbone of today's world, or should I say e-world. Its importance cannot be estimated, and as such, the security revolving around the software too is equally important if not more. This article would be describing a system whereby one of the biggest hindrances to the growth and expansion of the software industry, i.e. piracy, can be eliminated. The operative word being 'eliminated' and not 'reduced', which is why this system is so unique, unlike various other similar attempts made in the same area.

There have been several attempts in the making and designing of anti-piracy systems, be it on the software level or the hardware level. For example, there used to be a hardware serial key (an attachment say to the COM port) and the software used to "check " its presence before execution. The basic flaw here is that traditionally, softwares used to "check" for keys present as files or manually entered serials and here too it is the same simple "check". Thus, the "intruder" simply needed to emulate this "check" eliminating the presence of the key. There is no vast change in the implementation of software and hardware checks, its just that existing software protections have been ported to the hardware level making little or no use.

However, this system doesn't rely on any such "checks" and uses a completely novel approach. Infact, this system is so unique that it can easily be ported on to prevent DVD piracy, optimize internet security and so forth. However, the core of this product is to put a "economically viable" check on software piracy.

Hence, I put full emphasis to **not confuse this system to existing systems,** and, as far as I am aware of, there has been no duplicate or replicate of this system.

Concept :

The underlying concept behind the anti-piracy lock looks pretty simple, but as you go deeper and deeper, it becomes more and more complicated. The concept is that the lock acts as a hardware authentication device for the working of any software, and the software could be an Operating System, or just a simple little game. However, the lock does a 'little' more than just authentication, and this is where all the difference lies between the previous locks and this lock.

The Lock :

The lock is a hardware device which could be connected to your COM port or communication port.

The lock needs to have the following properties to enable its proper and secure functioning :

1. In Built Memory : To store various details with respect to the user. If function would be similar to a SIM card in a mobile handset.
2. Proper Authentication hardware logic : So that the device can validate the information that flows through it.
3. An Encoding / Decoding Unit : The heart of the device

Apart the above circuit components, the lock also consists of a LED which glows when the "key" has been properly authenticated.

The Key :

The key is an electronic hardware device which is to be inserted into the lock.The key contains the necessary authentication required for a given program to run. The exact working and nature of this key is one of the uniqueness of this anti-piracy device.

The Working Of the Lock:

The working or operation of the lock and key differs from the type of software it is protecting. The operation however can be summarised as follows :

For the Operating System

For the OS, ePolice offers a protection in tandem with the "critical files". This is another very unique aspect of the lock which indicates that the device doesn't need any kind of an operating system to run on. This essentially implies that the ePolice solution is platform independent.

For 3rd party software to be picked up off the shelf

The operation in a gist here is that the software comes with a hardware key. You simply enter the key into the lock and once the green LED gets illuminated, you remove the key. The software upon installation needs the appropriately authenticated lock for proper execution.

This is where the difference between previous attempts at hardware locks and this lock gets highlighted. Again, the technicals are beyond the scope of this synopsis .

For 3rd party software which can be downloaded:

This is the first and only hardware protection offered to files which can be downloaded from the internet. The features and operations of this lock facilitates this to be possible securely without infringing into any anti-privacy loopholes. The details are beyond this synopsis.

The Business Model :

As we are the manufacturers of this lock, we could give the lock as the part of an OS, in the sense that every OS manufacturer interested in protecting the piracy of its product would sign up with us and we would be making our lock for each copy of the OS.

Then, any 3rd party developer who is interested in our protection signs up with us and he orders "x" amount of keys from us for that particular software he has developed.

For 3rd party software (downloadable as shareware or trialware), our model changes a bit because there is no manufacturing of hardware keys here. However, to understand our pricing here, one should know the technicals of our protection .

Implementation of this device against DVD piracy or enhancing internet security is altogether another business model.

Legislation :

Congress has entered the arena that predominantly belonged to the software and hardware companies. Sen. Ernest Hollings, chairman of the Senate Commerce Committee, proposed one solution but kicked up a storm in March when he introduced a bill that would prevent new computers, CD players and other consumer-electronics devices from playing unauthorized movies, music and other digital-media files. The bill has been embraced by the various recording studios and other content producers though it has received little support from consumers and electronics manufacturers.

Also, there has always been a **conflict between "Piracy Laws" and "Privacy Laws."** Some anti-piracy measures have set ablaze several fights with the consumer advocates, one of the prime examples being **"sending user and software information to the company without permission and/or knowledge of the user."**

However, the solution proposed herein **doesn't involve sending of any information of the user to the company** or anyone. It will also **help roll the ball back into the court of the software and hardware companies and prevent Government intervention**. Such a solution will definitely be more acceptable to the consumers and hence also, would be more beneficial to the manufactures.

Final Words :

ePolice, as such is a hardware solution to the problems of piracy. However, as you may be knowing, there exists many hardware devices out there, more popularly referred to as a dongle, which due to some reason or the other have failed in not only getting the market but also keeping the security tight enough. To my knowledge, even the softwares with the most powerful dongles have suffered illegal copying.

ePolice essentially is not a dongle. And more importantly, it is the software which essentially ensures that ePolice unlike other dongles cannot be broken. **Thus even though it is a hardware device, its security is good because of the way the software is working in tandem.** Thats the one unique aspect. Secondly, ePolice doesn;t need the end user to change any hardware or software, **which means that exisiting software will work as usual.** Thirdly, **the target audience for the ePolice is not the PC vendors or the end-users, but the software developers themselves.** So, this ePolice system will directly cater to the needs of the software developer.

Also, ePolice doesn't violate any privacy laws as it doesn't need the user to transmit any information for necessary authentication, and also, it is not a device integrated with the PC which makes any kind of checks or adds its own digital signatures to users' files. **So, this system, if technically is not breakable, then should definitely serve as the best solution to software developers who need to protect their softwares and end-users who need to protect their data from being constantly monitored** which is done by current anti-piracy systems.

ePolice can be used for any type of software, be it an Operating System, a 3rd party application or a shareware downloaded from the internet. If this initial part of ePolice works successfully, then with some careful and simple engineering, it would be possible to extend the applications of ePolice to DVD Anti-Piracy, Digital signatures etc.

This might have been mentioned several times ago, and yet again it ought to be said again that **this synopsis is far too little to cover the technical aspects of this anti-piracy lock**. In fact, I would be more than happy to come and explain to you in detail each component of the lock, its working. implementation and applications. I have complete block diagrams of this electronic device with the analysis of each component. I would also be happy to tell you as to how this system could be used for various other security and piracy related subjects, such as DVD piracy, digital signatures, etc.

As my closing words, I would like to say that **this workable hardware – software model should in a great way enhance the fight to eradicate piracy, especially of computer softwares.**

Thanking you,
-Venkat Krishnaraj