CRYPKEY (CANADA) INC.

CrypKey Intelligent Hardware Sensing

CRYPKEY (CANADA) INC.

CrypKey Intelligent Hardware Sensing White Paper Revision 1.1

908 17 Avenue S.W. Suite 200
Calgary Alberta Canada
www.cypkey.com

Chapter

1

1. Introduction

CrypKey Intelligent Hardware Sensing is a feature that allows CrypKey to intelligently detect when software has been illegally copied to a different computer. This section introduces you to the CrypKey Intelligent Hardware Sensing System, and its features.

CrypKey (Canada) Inc. was the first license the concept of using the computer hardware to identify where software was licensed to run, thus eliminating the need for a dongle, and opening up the Internet as a way to instantly deliver software.

However, there were some drawbacks to this approach:

1. Not all computers had serialized information

2. Sometimes the information changed

3. Sometimes the information became briefly unavailable

These factors lead to situations where computers could not be licensed, and sometimes lost their license.

CrypKey Intelligent Hardware Sensing (CIHS) is designed to eliminate this kind of problem. By retrieving multipliable selected samples of hardware information, and intelligent detection of changes to this information, (CIHS) can differentiate between occurrences of the above situations, and illegal duplication of software.

Using this approach ahs the following benefits:

1. It is Robust – Since CIHS using multiple hardware samples, it can accept changes that may occur due to hardware change or error, without loss of license. This means less support calls.

2. It is Tolerant – CIHS can be configured to automatically relax security requirements for older machines that have less serialized information available (and less likely to have illegal copies). Again this means less support calls.

3. It is Adaptive: - As hardware parameters change, CIHS can adapt and actually add new information to its detection, maintaining an optimal level of security despite hardware changes. This means better protection from illegal copying, and less support calls.

4. It is Dynamic – Other hardware parameters can easily be added to CIHS as they become available due to future changes in computer hardware, or vendor proprietary hardware.

   Also, CIHS can be instructed to change the "what and how" of hardware it uses at any time, allowing the vendor to increase security or increase tolerance, even on a licensed machine. CIHS can conditionally allow the changes only if the license remains valid.

   This means future increasing security and robustness, and the vendor can adjust to choose the balance of security and tolerance that is right for them.

Chapter

2

2. CIHS Behaviour

CrypKey Intelligent Hardware Sensing is a new feature that is built in to CrypKey, and can be used seamlessly with no changes to your current code.

CIHS functionality is built in to CrypKey with reasonable default settings. No software changes are actually required to activate and begin using and benefiting from this feature. It is completely compatible with existing CrypKey licenses, and when an application with CIHS sees a license from a previous version of CrypKey, it will automatically switch it over to the CIHS security if possible with no loss of license.

To explain the behaviour of CIHS some simple concept are required.

2.1 Computer Hardware Identification Concepts

2.1.1 There is No Perfect Computer Serial Number

Many have searched for the holy grail of computer identification, but the answer has always been – it doesn't exist., for the following reasons:

- There is no standard that everyone must implement for this
- There are many manufactures, and they don't all implement hardware the same way
- There is a serial number inside some newer processors, but due to public privacy concerns, most manufacturers disable the this.
- There is a serial number on most newer drives, but no standard API to get at it. Unorthodox and undocumented methods have been somewhat successful, but sporadically fail.
- There is a PC serial number on most newer hardware, but some manufacturers fail to populate it, and it can, with difficulty, be changed.
- There are less serial numbers possibilities to be found on older computers.

For this reasons, identifying a computer is not an exact science.

2.1.2 Hardware Verification Results

CIHS will gather information from the hardware and each individual item of hardware is called a

Hardware Parameter. There can be 2 results of the information gathering for each Hardware Parameter:

a) **Retrievable** – CISH could read the information for the Hardware Parameter successfully
b) **Irretrievable** – CISH could read not the information for the Hardware Parameter successfully.

CIHS will then compare the information to previously recorded information, and the following 2 results are possible for each Hardware Parameter:

a) **Matched** – the gathered information is the same as previously recorded information.
b) **Unmatched** - the information was irretrievable, or the gathered information is not the same as previously recorded information.

If the CIHS decides the information it gathers, the hardware is the same hardware the software is authorized to run on, the hardware is said to be **Validated.**

2.1.3 False Positive, False Negative

The ambiguity in identifying a computer gives rise to 2 undesirable possibilities when identifying a computer for licensing purposes:

a) False Positive – in this situation, the software has identified the computer as the one it authorized to run on, when in reality, it is not. This means the software has been successfully illegally copied. For example, this might happen if the software relied on only the Volume name of the drive, and the attacker changed the Volume name to match the authorized computer.

The consequence of this is possible loss of revenue, if the attacker would have paid for the software had he been unsuccessful in copying it.

b) False Negative - in this situation, the software has identified the computer as one it is not authorized to run on, when in reality, it is. This means that the customer has been unjustly denied access to the software.

The consequences of this are many:
- customer dissatisfaction
- loss of revenue due to returned sale
- loss of revenue due to support calls

2.1.4 Security vs. Compatibility

Two configurable elements of CIHS are:

a) the number of Hardware Parameters required to be matched for hardware to be Validation
b) the number of Hardware Parameters that can changed but hardware is still Validated

The False Positive/Negative possibilities give rise to direct opposition in two desirable factors to consider when making choices about licensing, and how to configure CIHS:

a) Security – The higher the security in this area, the less likely hardware can be duplicated, and software illegally copied..

Higher security can be achieved by:

i) requiring that a higher number of Hardware Parameters are matched.
ii) requiring a lower number of Hardware Parameters are allowed to change.

However, these requirements increase the chances of a False Negative, and are therefore in opposition to compatibility.

a) Compatibility – The higher the compatibility in this area, the more likely hardware can be duplicated, and software illegally copied. Higher compatibility can be achieved by:

i) requiring that a lower number of Hardware Parameters are matched.
ii) allowing a lower number of Hardware Parameters to change.

However, these requirements increase the chances of a False Positive, and are therefore in opposition to security.

2.2 Points to consider on Security Settings

There are some points that should be considered when setting the behaviour of a feature such as CIHS.

To get the optimal behaviour, there is a fine line to walk between too opposing requirements: security, and compatibility.

Security is desired to prevent illegal duplication due to the following situations:

a) Your application is likely to be copied by people who would otherwise pay for it
b) Your application is going to be distributed in a high piracy geographical area (such as China, Russia)
c) Your application has a high selling price
d) Your application is widely distributed

However, high compatibility is desired to prevent locking out paying customers due to the following situations:

a) Your application has a wide distribution, with many customers
b) Your application is mission critical to customers
c) You don't have the resources to handle the higher level of support that comes with higher security

A careful analysis of the gains vs. the losses of security is required for a feature such as CIHS to be successful.

2.3 CIHS Security Settings

The following is some of the hardware verification logic implemented in CIHS:

2.3.1 Minimum Number of Hardware Parameters

This setting selects the minimum number of Hardware Parameters that are required to be retrievable before the computer can be licensed. If this number is not achievable on any particular machine, it will not be allowed to be licensed. This setting most directly controls the security vs., compatibility characteristics of CIHS behaviour.

2.3.2 Desired Number of Hardware Parameters

This setting selects the number of Hardware Parameters that are required to be retrieved before CIHS can stop retrieving any further Hardware Parameters. This can be considered a “soft minimum”, as CIHS will attempt to get this number if it can, but if not, allow the computer to by licensed using the “Minimum Number of Hardware Parameters”. This setting gives the CIHS its adaptability, allowing it to ramp up security on newer machines, yet be compatible with older machines.

2.3.3 Maximum Change

This setting specifies how many Hardware Parameters can change in a single check, after which the Hardware is deemed not valid. Hardware Parameters can change naturally due to hardware change or failure, and this setting allows CIHS to be tolerant of these changes.

2.3.4 Priority Order of Hardware Parameter Gathering

This setting selects which Hardware Parameters are gathered and the order in which they are gathered. The CIHS system will stop gathering once the Desired Number of Parameters have been gathered. This setting can be used have fine control over what and how much information is gathered; allowing you to configure CIHS to try to get what you believe is the optimum information to provide the best security. The beneficial attribute of this setting is that:

1. If CIHS can retrieve the higher priority Hardware Parameters, which may be likely for most machines, it will, allowing optimum security where possible.

2. If CIHS can’t retrieve the higher priority Hardware Parameters, which may be the less likely case, it can still license the computer using lower priority parameters, allowing compatibility when required.

2.3.5 What Security Setting values does CIHS use?

CrypKey has used its many years of experience, as well as many many hours of testing, to devise what we consider to be optimal settings that balance perfectly both Security and Compatibility.

What are the Security Setting values? That is something we consider to be our secret recipe – something like Kentucky Fried Chicken ☺ .

However, you can be sure that CrypKey is applying both the technology, and the experience, to give you the best of both worlds in copy protection – Security and Compatibility.

3. Conclusion

This white paper discussed problems that arise when locking software to computer hardware to prevent illegal duplication.

It points out that there is no perfect hardware value to lock software to, and this gives rise to the possibility of either locking out paying customers, or allowing illegal copying of your software.

The paper goes on to describe elements of a system that uses multiple hardware values to make an intelligent decision as to whether software has been copied to a different computer.

CrypKey has used its many years of experience, as well as many hours of testing, to apply these elements to make an intelligent hardware sensing feature with optimal settings that balance perfectly both Security and Compatibility.

Chapter 3