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 software security company to license the concept of using computer hardware to identify where software was licensed to run. This approach has two main advantages:

1. Eliminates the need and cost for dongles.

2. Takes advantage of the power and convenience of the Internet as a way to instantly deliver software.

However, there were some drawbacks to this approach:

1. Not all computers have serialized information.

2. Sometimes the hardware identification information changes.

3. Sometimes the hardware identification information is briefly unavailable.

The above drawbacks lead to situations where a computer cannot be licensed, or loses its license for some reason.

CrypKey Intelligent Hardware Sensing (CIHS) is designed to eliminate the above licensing problems. By retrieving multiple selected samples of hardware information, and intelligently detecting changes to this information, (CIHS) can compensate for hardware anomalies and deliver a consistent and predictable copy protection and licensing solution.

Using CrypKey's CIHS hardware detection system has the following added benefits:

1. It is robust – Since CIHS uses 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 therefore less likely to have illegal copies). Again this means less support calls.

3. It is dynamic: - CIHS settings can be changed accordingly to maintain an optimal level of security despite hardware changes. 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 vendors can choose the balance of security and tolerance that is right for them and their customers.

4. This means more consistent protection from illegal copying and less support calls due to license issues.

5. It is adaptive –Hardware parameters can easily be added to CIHS as required including future changes to computer hardware and vendor proprietary hardware.

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 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 over to CIHS security with no loss of license.

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

2.1 Computer Hardware Identification Concepts

2.1.1 There is No Perfect Computer Serial Number

Many software engineers 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.
- There are many hardware 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 them.
- 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 these 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** – CIHS could successfully read the information for the Hardware Parameter
b) **Irretrievable** – CIHS could not successfully read the information for the Hardware Parameter.

CIHS will then compare the information to previously recorded information, and the following two 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 CIHS decides from the information it has gathered that the hardware is the same hardware that the software is authorized to run on, then the hardware is said to be **Validated.**

2.1.3 False Positive, False Negative

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

a) **False Positive** – The software has identified the computer as the same machine it is 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** - 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 profitability 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 validation.
b) The number of Hardware Parameters that can change without affecting hardware validation.

The following two factors – Security and Compatibility – are in direct opposition and therefore must be weighed carefully when making a decision about how to configure the CIHS elements:

a) **Security** – The higher the security setting, the less likely hardware can be duplicated, and software illegally copied. Higher security is achieved by:

i) Requiring that a higher number of Hardware Parameters are matched.
ii) Allowing a lower number of Hardware Parameter changes.

Increasing security increases the chance of a False Negative therefore decreasing compatibility

b) **Compatibility** – The higher the compatibility setting, the more likely hardware can be duplicated, and software illegally copied. Higher compatibility is achieved by:

i) Requiring that a lower number of Hardware Parameters are matched.
ii) Allowing a lower number of Hardware Parameter changes.

Increasing compatibility increases the chance of a False Positive therefore decreasing security.

2.2 Points to consider on Security Settings

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

The following should be considered when setting the behavior of the CIHS feature:

1. 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 into a high piracy geographical area (such as China or Russia)
   c) Your application has a high selling price
   d) Your application is widely distributed

2. High compatibility is desired to prevent locking out paying customers due to the following situations:

   a) Your application has a wide distribution to 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 successfully implemented

2.3 CIHS Security Settings

This section describes the hardware verification logic implemented within 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 achieved on a 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, while still being 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 offers a fine level of control over what and how much information is gathered; allowing you to configure CIHS to achieve optimum security. The benefits of the Hardware Parameter setting are:

1. Optimum security by CIHS retrieving the higher priority Hardware Parameters when they are available.

2. Next best level security if CIHS can't retrieve the higher priority Hardware Parameters. CIHS will still license the computer using available lower priority Hardware 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 man 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? They are considered to be our industry advantage and therefore our secret formula. Only our customers can take advantage of this formula today!

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.

Chapter 3

3. Conclusion

This white paper discussed issues that arise when locking software to computer hardware to prevent illegal duplication. There is a fine balance between Optimum Security and Compatibility. At one end of the spectrum security can be so rigid that it has the possibility of locking out paying customers. At the other end of the spectrum security can be so weak that it doesn't deter illegal copying of software.

The paper described elements of CrypKey's newest protection 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.