HiGate (High Grade Anti-Tamper Equipment) Prototype and Application to e-Discovery

Yui Sakurai
The Dept. of Information Systems and Multimedia Design
School of Engineering
Tokyo Denki University
2-2 Kanda-Nisikicho, Chiyoda-Ku, Tokyo, 101-8457
Japan
sakurai@isl.im.dendai.ac.jp

Yuki Ashino
NEC Corporation, Service platform Institute

Tetsutaro Uehara
Associate Professor
Academic Information Media Center
Kyoto University

Hiroshi Yoshiura
Professor
The University of Electro-Communications

Ryoichi Sasaki
Professor
Tokyo Denki University

ABSTRACT

These days, most data is digitized and processed in various ways by computers. In the past, computer owners were free to process data as desired and to observe the inputted data as well as the interim results. However, the unrestricted processing of data and accessing of interim results even by computer users is associated with an increasing number of adverse events. These adverse events often occur when sensitive data such as personal or confidential business information must be handled by two or more parties, such as in the case of e-Discovery, used in legal proceedings, or epidemiologic studies. To solve this problem, providers encrypt data, and the owner of the computer performs decoding in the memory for encrypted data. The computer owner can be limited to performing only certain processing of data and to observing only the final results. As an implementation that uses existing technology to realize this solution, the processing of data contained in a smart card was considered, but such an implementation would not be practical due to issues related to computer capacity and processing speed. Accordingly, the authors present the concept of PC-based High Grade Anti-Tamper Equipment (HiGATE), which allows data to be handled without revealing the data content to administrators or users. To verify this concept, an e-Discovery application on a prototype was executed and the results are reported here.

Keyword: Anti-Tamper, e-Discovery, Bitlocker, APIHook

1. INTRODUCTION

These days, most data is digitized and processed in various ways by computers. In the past, computer owners were permitted to process data as desired and to observe the inputted data and the interim results. However, the unrestricted processing of data and accessing of interim results even by computer users is associated with an increasing number of adverse events. These adverse events often occur when sensitive data such as personal or confidential business information must be handled by two or more parties, such as in the following cases.

1. (1) Epidemiologic studies: Epidemiologic studies often seek to compare data concerning (a) physical loads, such as the exposure dosage of individuals at a workplace and (b) the incidence of illnesses, such as cancer, obtained from hospitals and field studies for investigating correlations with various factors. However, when this data is transferred to a partner or third party and the usual processing is performed, personal information contained in the inputted data or interim results may be revealed to the person using the computer to perform the data processing. This is a problematic situation from the standpoint of protecting personal information. Consequently, at present, the exchange of this data is not possible, thereby creating a problem in that epidemiologic studies cannot be used to improve the health of citizens. As a current solution, (i) data encrypted by the original owner may be transferred to a partner or third party, and (ii) the partner or third party may input the encrypted data into a computer, which after the data is decrypted, implements certain processing and outputs only correlation values, so that the interim results and other sensitive information are not accessible to even the computer user.

2. (2) e-Discovery: Japanese companies are often involved in e-Discovery performed for US civil court. Prior to preceding to trial in a US civil court in both Japanese and US civil courts the defendant and the plaintiff sides mutually disclose electronic evidence. At this time, if electronic documentary evidence containing a keyword or other security mechanism by the plaintiff side exists but is not disclosed, the trial will be severely disadvantaged. Conversely, if all accumulated electronic data is

> disclosed unconditionally, personal information may be revealed and critical business information may be leaked unnecessarily to a rival plaintiff. For this reason, electronic documents may be partially sanitized [4]. The plaintiff side receiving the sanitized electronic documents may want to verify with a computer that the sanitized portions do not contain keywords, but if viewing the sanitized portions is freely permitted, the defendant-side secrets would be revealed unfairly. To resolve these problems, computer processing may also determine whether the sanitized portions contain keywords, but other processing such as deciphering the sanitized portions should not be performed, and the interim results should not be revealed.

Common to the solutions of these problems is that the computer owner performs only specific processing of the data and is able to observe only the final results. One conceivable means to realize such a solution is to use tamper-resistant equipment that prevents the owner from changing the processing or accessing interim results. Smart cards (also known as IC cards) are typically used as the tamper-resistant equipment. A smart card contains a secret key that is not revealed, even to the user, and public key encryption, which is generally used to implement digital signatures.

Smart cards, however, have the problems of slow processing speed, small memory, and are difficult for an average person to program using an ordinary computer language. Thus, we developed a system that overcomes these problems by improving the PC hardware and software. This new system, configured from PC-based hardware and from software such as the boot control function (BCF) [11] previously developed by the authors, is known as High Grade Anti-Tamper Equipment (HiGATE).

This paper presents the HiGATE concept, and reports the results of the application of a prototype to e-Discovery.

With the heightened interest in the handling of personal and confidential information, the range of applications for HiGATE is expected to increase in the future.

To achieve the same objective, the use of an encryption protocol has also been envisioned, but such an approach would only be suitable for an extremely narrow range of applications and could not be applied to the types of problems encountered here. Approaches similar to that used in our research, that is, preventing even a computer user from freely processing data and accessing interim results, have not been reported in other studies.

2 OVERVIEW OF PROPOSED SYSTEM

2.1 HiGATE Requirements

HiGATE has the following five requirements.

1. A tamper-resistant area exists that even the owner cannot access.
2. A memory with sufficient capacity for calculations is provided
3. Arithmetic computations are processed at a fast speed.
4. Programming by a trusted third-party, rather than the owner, is permitted.
5. The equipment is easy to realization.

A smart card is an example of a device capable of satisfying the first requirement above. The use of a smart card, however, has the following two problems. First of all, the processing capacity presents a problem, especially in cases such as e-Discovery, where large quantities of data are handled and processing must be done within a limited timeframe. Secondly, programming a smart card requires the use of special techniques such as micro-programming, and an ordinary person would not be able to program a smart card as desired. Thus, the development of HiGATE, which satisfies the above five requirements, was needed for applications not suitable for smart cards.

2.2 Measures for Satisfying the Requirements

(Requirement 1)

The HiGATE functions necessary to satisfy requirement 1 are listed below:

① Hardware function

Capability to prove that the equipment case has not been opened

② Software functions

1. Boot control function for application programs
2. Encryption function for entire hard disk (HDD)
3. Arithmetic processing function
4. File delete function that leaves intact the inputted data for calculations and the interim results.

These functions are described in detail in Section 3.

(Requirements 2, 3, 4 and 5)

Requirements 2, 3, 4 and 5 can be implemented automatically through the process of PC-based development. In other words, PC-based development provides the advantages of fast I/O throughput and computational speeds, the capability to accumulate large quantities of data, and the ability to use a common programming language such as C or JAVA instead of a special programming language. Moreover, PC-based development facilitates installation since there is no significant need for special equipment. In this case, Windows, with which the authors have much experience, was chosen as the OS.

3. HIGATE CONFIGURATION

3.1 Prerequisites

(Prerequisite 1) The BIOS and OS are running properly.

(Prerequisite 2) Unauthorized actions are not performed when implementing the HiGATE settings.

(Prerequisite 3) HiGATE does not contain an unauthorized program.

HiGATE operates under the abovementioned conditions.

3.2 Possible Unauthorized Actions

There are three conceivable methods for attacking HiGATE, and these are listed below:

1. (Unauthorized action 1) Forcible opening of the case and extraction of information from the memory
2. (Unauthorized action 2) Removal of the HiGATE HDD and connection to another PC to extract the HiGATE internal data and programs, etc.
3. (Unauthorized action 3) Activation of an unauthorized program to modify other programs or steal information.

3.3 Functions to Protect Against Unauthorized Actions

(Protection 1) Provide proof that the case has not been opened.

As in the description of unauthorized action 1, it is conceivable that the case can be opened and the memory contents stolen. Accordingly, it is important to prevent the case from being opened. This protection may be realized by the following two methods.

1. Cause the power supply or other essential device to shut off and the memory contents to disappear if the case is forcibly opened. Methods for switching off the power supply include: (a) microswitch-based detection of the case opening, (b) detection via a lead switch and a magnet on the case cover, and (c) optical detection of the lid opening.
2. Provide a seal that clearly indicates whether the case has been opened. Tamper-resistant labels are an existing technology. If a tamper-resistant label is peeled off, an indication that the case has been opened remains. By making the data contained in the HiGATE lose its effectiveness when a seal is cut and peeled off, unauthorized actions by the user can be prevented.

Here, we decided to use method (2), which is easily achieved. In the future, a combination of methods (1) and (2) will enable enhanced safety.

(Protection 2) HDD encryption

HDD encryption is implemented to prevent the HDD used in the HiGATE from being removed or connected to another PC and to prevent the HDD contents from being modified or extracted as described in unauthorized action 2. An existing technology is the BitLocker function which is provided only in Windows Vista Enterprise and Windows Vista Ultimate editions. Because Windows Vista Enterprise is only sold through volume licensing, we installed Windows Vista Ultimate as the HiGATE OS.

(Protection 3) Boot control (BCF/Vista)

As described in unauthorized action 3, it is conceivable that an unauthorized program can be activated to modify other programs and steal information. BCF/Vista [11] is an existing technology developed by the authors to prevent such unauthorized actions. The BCF/Vista function is described in detail in Section 3.4.

Other functions include the file delete and arithmetic processing functions. The file delete function deletes data from the HDD used with HiGATE. This function operates so that the HiGATE user does not leave behind any data after the usage of that data has been completed. The HiGATE system handles data which even the user is not permitted to view. Accordingly, the continuous retention of data in the user’s HiGATE system will lead to an unauthorized action. The arithmetic processing function is used in different ways depending on the application, and can be developed freely by the program developer. Additionally, unauthorized actions through the skillful use of the keyboard are conceivable, but can be avoided through the use of the device driver installation control function in Windows Vista Ultimate.

3.4 BCF/Vista

BCF/Vista was a part of the development of the Dig-Force [2][3] digital forensic system.

BCF/Vista computes hash values for programs that are activated during setup, registers these hash values in a white list, and digitally signs the entire white list. The OS and then BCF/Vista are set to start next. After they are running, the BCF/Vista function computes hash values for application programs as they try to start up, and after confirming the validity of the previously registered white list by signature verification, the computed hash value is compared to the hash value in the white list. If the value is the same as the registered hash value, the program starts, but if not registered, APIHook is used to prevent the program from starting.

As a result, even if an unauthorized program attempts to start up, if Prerequisite 1 that “the BIOS and OS are running properly,” has been established, the unauthorized program can be prevented from running. For further details regarding the BCF/Vista function, refer to reference document [11].

3.5 Functional Configuration

Providing the hardware function and the four software functions listed in Section 2.2 enables a tamper-resistant area to be realized to protect the OS and the arithmetic processing function residing on the HDD, as well as the keys, data, etc., residing in memory. Accordingly, an arithmetic processing program created by a program developer and placed in the tamper-resistant area can be executed correctly by the HiGATE system without any unauthorized actions. The HiGATE functional configuration is shown in Figure 1 and smart card and HiGATE functions are compared in Tables 1 and 2.

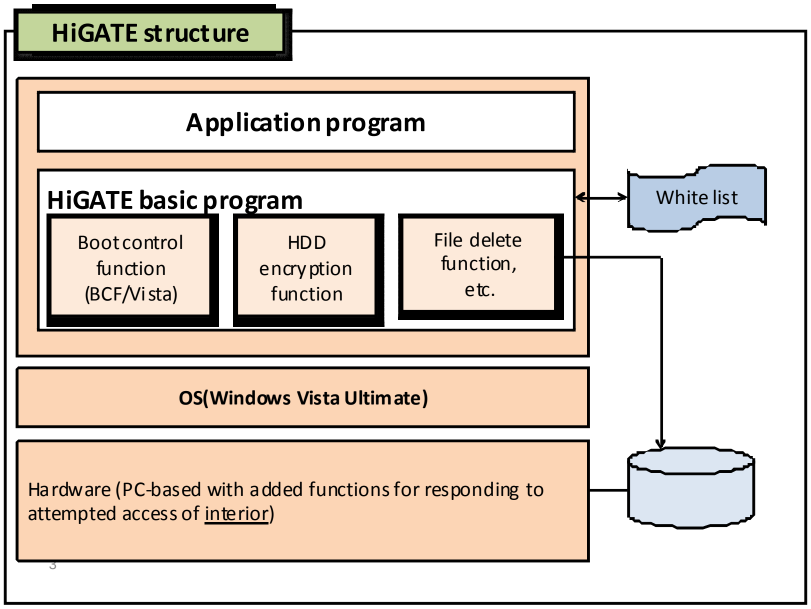
HiGATE structure
Application program
HiGATE basic program
Boot control function (BCF/Vista)
HDD encryption function
File delete function, etc.
White list
OS(Windows Vista Ultimate)
Hardware (PC-based with added functions for responding to attempted access of interior)

Figure 1. HiGATE Block Diagram

Table1. Differences between Smart Cards and HiGATE

Difference	IC Card	HiGATE
OS	EMV specification	Windows Vista Ultimate
Limitation due to program language development	Limited	Not limited
Memory	RAM (1 MByte)	RAM (3 Gbytes)

Table 2. Similarities between Smart Cards and HiGATE

Similarity	**IC Card**	**HiGATE**
Startup of predetermined program	Read-only semiconductor memory	BCF/Vista
Memory cannot be accessed externally	Encryption circuit or single-chip implementation of memory	Case cannot be opened with tamper-resistant label
False environment cannot be created	Access controlled by CPU	HDD encryption
Tamper-resistant area	Access controlled by CPU	・BCF/Vista ・HDD encryption ・Tamper-resistant label

4. HIGATE OPERATION

This section describes the HiGATE operation:

① HiGATE manufacturing phase
② Program installation phase
③ Setting phase
④ Usage phase.

Persons involved in the above four steps of HiGATE operation include the manufacturer, program creator, and user.

① Manufacturing phase

The manufacturer preinstalls the OS (Windows Vista) and BCF/Vista required for HiGATE in the HiGATE PC, and then transfers the HiGATE system to the program developer.

② Program installation phase

The program developer receives the HiGATE system from the manufacturer, and loads the processing programs necessary for application into HiGATE.

③ Setting phase

After program installation, the HiGATE system and BCF/Vista are configured with the necessary settings. At this time, the program creator implements the settings with administrator privileges.

(1) BIOS settings

To prevent booting of an OS installed on the PC other than Windows Vista, “Set the BIOS password” and “Restrict bootable storage to the HDD” BIOS settings are implemented, and only the program creator knows the BIOS password.

(2) User account settings

So that the operator cannot operate Windows services and the task scheduler from the user account that is utilized when operating the PC, the user account is not given administrator privileges.

(3) Program installation

Controller program files that comprise BCF/Vista, agent program files, and the white list files are installed. These files are stored on a drive encrypted by BitLocker (described below), and are set as read-only files that cannot be overwritten or deleted by the user account.

(4) BitLocker settings

BitLocker is a drive encryption function of Windows Vista Ultimate. BitLocker is used to encrypt all the drives on an HDD so that an attacker is unable to remove the HDD from the PC and use another PC to modify the programs that comprise BCF/Vista.

(5) Windows service settings

Nanshiki Corp.’s sexe freeware was used to register the controller as a Windows service. This service was registered under the name MonitoringController (hereafter referred to as MC Service). As a result, the controller starts up automatically after Windows Vista has started. With this setting, however, MC Service will not start if the user account is logged in while in safe mode. Therefore, MC Service information is added to the Windows registry so that MC Service will start even in safe mode.

(6) Task scheduler settings

The task scheduler is used so that startup occurs when an agent logs into the user account.

After implementing these six settings, tamper-resistant labels are affixed to all HiGATE parts that could be opened.

④ Usage phase

The user uses a HiGATE system which has been set up as above. At this time, a user account that does not have administrator privileges is used by the user.

These are the phases of HiGATE operation. By allocating the above roles to the participants involved, the participants can be prevented from performing any unauthorized actions. HiGATE users do not possess administrative privileges, and therefore it would be difficult for them to perform an unauthorized action on the data. Moreover, since the program creator does not possess the HiGATE system, it would be nearly impossible for him or her to implement an unauthorized action on the data handled by the user. Accordingly, none of the participating individuals are able to perform an unauthorized action on the data used and handled by the HiGATE system. The prerequisite that the BCF/Vista administrator does not perform any unauthorized actions is made possible by this system.

5. APPLICATION TO E-DISCOVERY

In this section, the HiGATE system is applied to e-Discovery. The e-Discovery system described is the "e-Discovery System for Sanitizing Disclosure Information and for Securing Evidence" [1] proposed by Takatsuka et al.

5.1 e-Discovery

The US Federal Rules of Civil Procedure (FRCP) were amended in December 2006 so that in US civil litigation, corporations are obligated to disclose electronic evidence during the discovery phase held before the start of a civil trial. This disclosure of electronic evidence is known as e-Discovery [5][6][8]. Figure 2 shows the basic flow of the e-Discovery procedure.

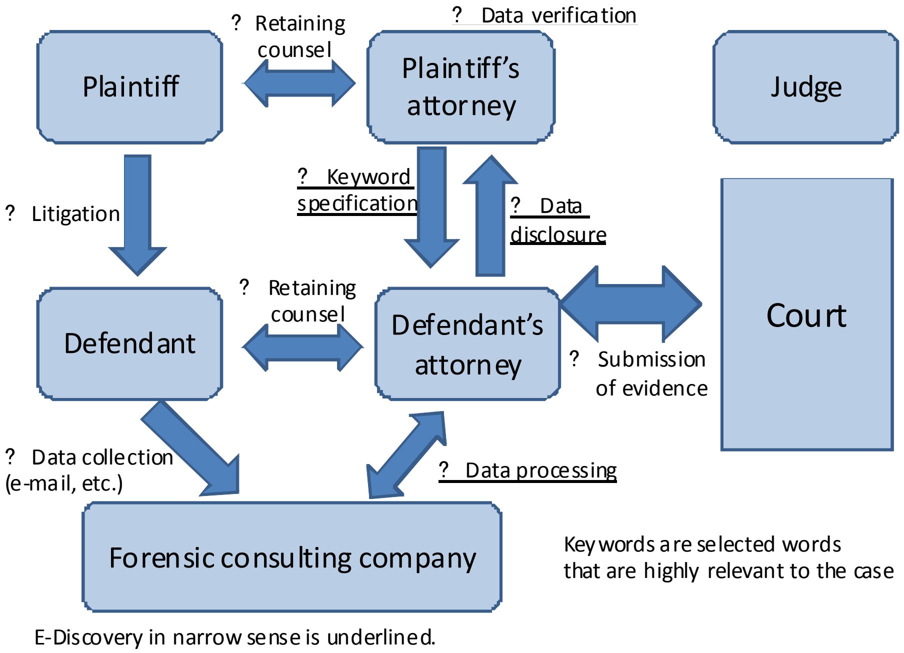

Figure 2. e-Discovery Procedure

5.2 e-Discovery System Proposed by Takatsuka et al.

First, the plaintiff side provides the defendant side with keywords which relate to the case. Then, using those keywords, the defendant side discloses files relating to the case. However, these files may include information such as company secrets that the company does not want to disclose. As a solution, electronic sanitizing technology [4] is used. The defendant side completely sanitizes documents that do not contain keywords, and partially sanitizes documents that contain both keywords and passages which the company does not want to disclose. This method permits the disclosure of only the minimum required data. With the present sanitization technology, however, a keyword may be contained in an area to be sanitized, and verification thereof is nearly impossible. Takatsuka et al. solved this problem by encrypting the data contained in a sanitized area. Data that has been subjected to sanitization with encryption is disclosed to the plaintiff side. The plaintiff side accepts and verifies the data. At that time, the plaintiff side verifies that keywords are not contained in sanitized areas.

With this process, however, the decrypted results of sanitized locations may be unfairly observable. Therefore, a tamper-resistant security device is used so that interim results cannot be observed, and the HiGATE system is used for this purpose. Here, a HiGATE system that includes the program part developed for e-Discovery is referred to as HiGATE/e-Discovery.

We developed the minimum needed programs for HiGATE/e-Discovery. The languages used are C# and C++, and constitute a total of approximately 3,000 steps.

5.3 HiGATE/e-Discovery Operation

This section describes the operation when HiGATE is applied to e-Discovery. HiGATE is used as a security device at the application site. Application of the HiGATE system solves the problems of data interference by the plaintiff side and the slow processing speed associated with smart cards.

1. HiGATE/e-Discovery manufacturing and program loading

   The manufacturer transfers the HiGATE system to the program developer. The program developer loads e-Discovery software into the HiGATE system. The e-Discovery software program has five functions for digitally verifying keyword files, decrypting sanitized passages, verifying whether keywords exist in a decrypted passage, verifying evidence, and extracting files relating to the case.

2. HiGATE/e-Discovery settings

   The HiGATE settings were described in Section 4. e-Discovery keywords are also delivered and the plaintiff and defendant sides exchange public keys.

3. HiGATE/e-Discovery usage

   The plaintiff side inputs the data received from the defendant side into HiGATE/Discovery, and runs the program. This enables the plaintiff side to verify that keywords are not contained in the sanitized areas. Next, the plaintiff side reviews only the data related to the case, and moves ahead with the litigation.

Based on these considerations, the applicability of HiGATE to e-Discovery appears promising.

6. CONCLUSION

This paper has proposed hardware that is equipped with a tamper-resistant function that cannot be modified by even the hardware owner, has fast I/O throughput and arithmetic processing speeds; is capable of accumulating large quantities of data that can be programmed similarly to a PC and can be developed inexpensively and easily. A prototype was built and the results of an application of e-Discovery were reported.

The basic HiGATE program developed this time has only minimal functionality, but we intend to expanded the functionality in the future, and improve the ease-of-use and safety.

The HiGATE system is suitable for application to situations requiring technology for proving that an administrator has not accessed files or participated in the processing. In addition to e-Discovery, the application is thought to be possible in many other fields, such as data matching in an epidemiologic study.

REFERENCES

[1] Mitsuyuki Takatsuka, Masataka Tada, Ryoichi Sasaki, “Proposal of the e-Discovery System for Sanitizing Disclosure Information and for Securing Evidence”, The 2007 International Workshop on Forensics for Future Generation Communication Environment (2008)

[2] Yuki Ashino,Ryoichi Sasaki, “Proposal of Digital Forensic System Using Security Device and Hysteresis Signature”, The Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2007)

[3] Keisuke Fujita, Yuki Ashino, Tetsuro , Uehara, Ryoichi Sasaki, “Proposal of Digital Forensic System with a Boot Control Function against Unauthorized Programs”, 4th Annual IFIP WG11.9 Conference on Digital Forensics (2008)

[4] Kunihiko Miyazaki, seiichi siozaki, Mituru Iwamura, Tsutomu matsumoto, Ryoichi Sasaki, Hiroshi Yoshiura, “The issue of electronic document sumi coating”, ISEC2003-20, pp61-67 (2003)

[5] e-WORD Digital Forensic, “digital forensics”, http://e-words.jp/w/E38387E382B8E382BFE383ABE38395E382A9E383ACE383B3E382B8E38383E382AF.html, (2008.2)

[6] Ji2 eDiscovery : Service outline, http://www.ji2.co.jp/service/ediscovery/, (2008.2)

[7]Ryoichi Sasaki, “@police No. 8 security commentary digital Forensic, ”http://www.cyberpolice.go.jp/column/explanation08.html, (2008.2)

[8] EnCase, “About e-Discovery”, http://www.encase.jp/glossary/eDiscovery.html(2008.2)

[9] Mitsuru Iwamura, Kunihiko Miyazaki, Tutom Matsumoto, Ryoichi Sasaki, Takeshi Takeshi, “Pass with the issue of alibi proof in the e-signature; the issue of time proof－A hysteresis signature and the concept of digital ancient documents－”, Computer science magazine bit Vol32, No11 (2000)

[10] Ron.Steinfeld ,Laurence.Bull,and Yuliang.Zheng, "Content Extraction Signatures", ICISC 2001, pp285-304(2001)

[11] Yuki Ashino, Keisuke Fujita, Maiko Furusawa, Tetsuro Uehara, Ryoichi Sasaki, “Extension and Evaluation of Boot Control for a Digital Forensic System”, 5th Annual IFIP WG11.9 Conference on Digital Forensic (2009)