3-13 A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave

TANAKA Hidema, TAKIZAWA Osamu, and YAMAMURA Akihiro

This paper describes the experiments and analysis of the interception of personal computer's display image using emanation of electromagnetic wave. We used personal computers as the targets and experimented on reconstruction of screen information under the following equipments and environments; (1) using a near magnetic field probe, (2) using an antenna from away place, (3) using an injection probe over power supply cable. From the result of (1), we show that the slight difference in the synchronous frequency of video signal among PCs will become the key which recognizes the target. In the experiment (2), we succeeded from about 4 meters away place with frequency which is inside of VCCI regulations. In the experiment (3), we succeeded from about 30 meters away place, and we found that the position relation between a probe and AC adapter is dependent on results.

Keywords
Electro-magnetic wave, Side-channel attack, TEMPEST, Security, EMC

1 Introduction

In recent studies on encryption and other information security technologies, more researchers are focusing on countermeasures against attacks aimed at gaining confidential information by methods other than electronic eavesdropping on communication channels. In "side-channel attacks", attackers intercept information revealed unintentionally through physical processes or gain confidential information by exploiting hardware defects. Side-channel attacks are classified depending on whether attackers establish access to attack targets, and on whether attackers sabotage attack targets to cause the targeted devices to operate in ways other than originally intended [1]. Various physical properties are exploited by attackers for side-channel attacks, including the amount of power consumed, emissions of light, electromagnetic waves, or ultrasonic waves, etc. Additionally, various methods of attack are available: methods in which no physical contact is made with the targeted device, destructive methods based on some mechanism within the device, and methods that involve some combination of the two. A key task when assessing these potential attacks is to measure observable physical properties in a realistic environment and to evaluate these properties in detail. In contrast with computation-theory security models, Micali and Reyzin have formulated and proposed a model of security against physically observable attacks that exploit information leaked from physical processes [2]. Their aim was to show, within a logical framework, the sort of cryptographic primitives that can be used to enable secure encrypted communication given certain observable physical properties. Achieving this aim requires measuring and confirming observable physical properties

in a real-world environment.

Electromagnetic waves are generated by the operation of equipment comprised of high-frequency circuits such as personal computers (referred to simply as "computers" below); these waves emanate from the equipment. Electromagnetic emissions can be considered to pose two threats to information security. First, there is the risk that signals may be intercepted during encryption processing, providing attackers a key in cryptanalysis. Second, in a risk unrelated to cryptanalysis, confidential user information may be intercepted directly.

This paper reports on the results of experiments on potential threats of the second type. If screen images on computers can be intercepted, confidential information from other computers on the network can also be intercepted, rendering network security policies powerless. Methods of intercepting screen images from CRT monitors and the like have been known for quite some time, and the methods themselves are regarded as highly confidential information. This consideration—and the fact that experimental results depend greatly on the equipment and environment, making quantitative analysis difficult—account for the scarcity of published documents featuring detailed procedures (including specific measurement values) and clear results. Specifically, it is indispensable that the quality and quantity of leaked data, the equipment, and methods of the experiment be clarified when discussing security that addresses the model of physically observable attacks proposed by Micali and Reyzin. Thus, in this paper we discuss the results of experiments using actual equipment, reporting on a procedure for intercepting electromagnetic waves that reveals computer-screen images. Our aim was to provide an index of technical factors involving the emission of the waves, the quality and quantity of leaked information, the cost of staging attacks, and the cost of defensive measures.

2 Classification of electromagnetic emission interception

Content subject to leaking and content subject to interception through electromagnetic emission are classified in terms of equipment input and output data. These are summarized in tables 1 and 2 [3]. In addition to screen images, keyboard strokes and printed text are also at risk of interception. This means, for example, that even passwords not displayed on-screen may be intercepted.

Table 1 *Interception of output information*

Leakage source	Leakage target	Example of becoming threat of interception object
PC, cable, and display	Content of display	Document and mail text etc.
Printer	Content of print	Classified document etc. under print
	Printing method	Model information etc. on printer material

Table 2 *Interception of input information*

Leakage source	Leakage target	Example of becoming threat of interception object
keyboard and cable	Content of key stroke	Login ID and password, etc.
Touch panel	Coordinate value	Reproduction of selection with touch panel and input information on specified type etc.

Screen images and keystroke signals in the final link of the human-machine interface on computers and other information and communication devices represent information provided directly to users. Thus, these signals cannot be encrypted, and if they are emitted as electromagnetic waves, conventional security protection technology cannot prevent interception. Proposals have thus called for device-based measures that maintain electromagnetic emissions from information and communication equipment below a prescribed level, as well as measures for electromagnetic shielding of buildings and more secure methods of equipment installation and setup [3].

3 Experimental equipment and targets

With respect to the means of interception described in Table 1, we conducted experiments to intercept electromagnetic emissions from computers and to recreate screen images from targeted computers. In the experiments, we used a Rohde & Schwarz FSET22 test receiver (Fig.1) and SystemWare FrameControl Ver. 4.24 as an image-processing application. The test receiver specifications are given in Table 3. FrameControl supports processing of input signals from the test receiver at 256 frames/3 sec. Real-time image processing is available by averaging up to 256 frames. As the near-magnetic field probe, an Anritsu MA2601B (frequency bandwidth: 5 MHz to 1 GHz) was used; as an antenna, an Anritsu MP666A log-periodic antenna (frequency bandwidth: 20 to 2000 MHz) was used; and as the injection probe, an NEC Tokin EIP-100 (frequency bandwidth: 80 kHz to 30 MHz) was employed (Figs.2 and 3). The MA2601B offers conversion coefficient values for magnetic field strength to measured voltage of 35 dB at 5 MHz, 12 dB at 100 MHz, 8 dB at 500 MHz, and 10 dB at 1 GHz [4]. Meanwhile, the MP666A offers conversion coefficient values for magnetic field strength to measured voltage of +3 dB at 100 MHz, -14 dB at 500 MHz, and -21 dB at 1 GHz [4].

We used desktop and notebook computers as interception targets. The experiments were conducted on desktop computers equipped with three types of video cards (ATI Radeon 9700, NVIDIA GeForce2 MX/MX400 PCI, and NVIDIA GeForce3 Ti500) and a notebook computer equipped with a graphics controller

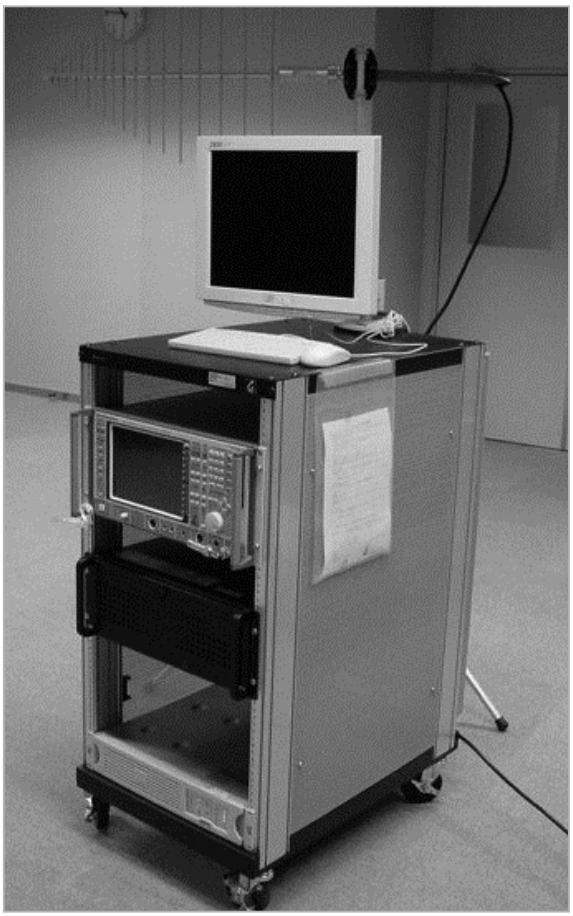

Fig.1 *Test receiver used in the experiments*

Table 3 *Specifications of test receiver used in the experiments*

Frequency range	10Hz ～ 22GHz
Frequency resolution	0.1Hz
Bandwidth	100Hz ～ 500MHz
Average noise level	-142dBm以下（1MHz）

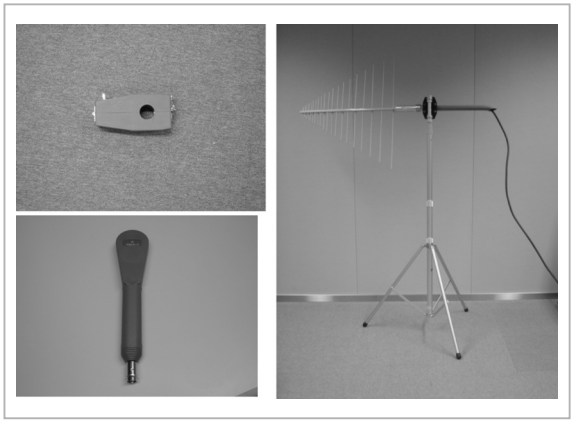

Fig.2 *Equipment used*

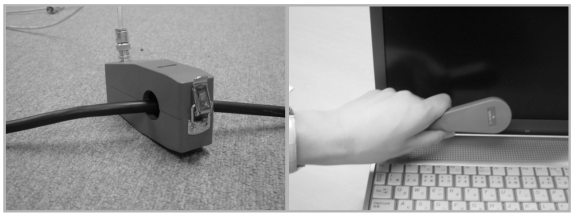

Fig.3 *Method used*

integrated in the motherboard (Intel 82845G/GL), for four different video processors in all. The desktop and notebook computers thus equipped are hereinafter referred to as “desktops” and “notebooks”, respectively. A Sony VAIO V505 was used as the notebook. For the displays, a Dell 16” LCD display (hereinafter, “LCD”) and a Nanao FlexScan 77F 21 21” CRT display (“CRT”) were selected. On the desktops, the screen depicted in Fig.4 was displayed and targeted for interception, and on the notebook, that of Fig.5 was displayed and targeted.

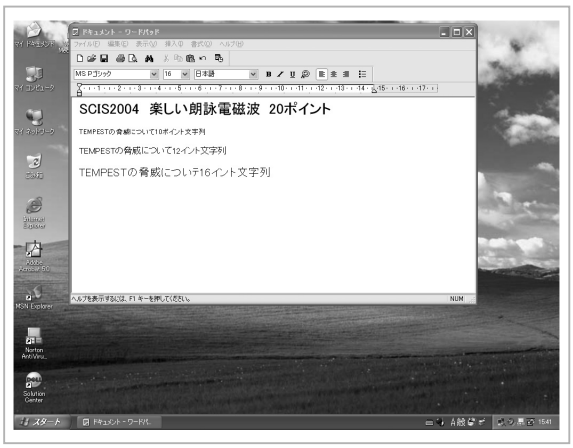

Fig.4 *Screen targeted for interception on the desktops*

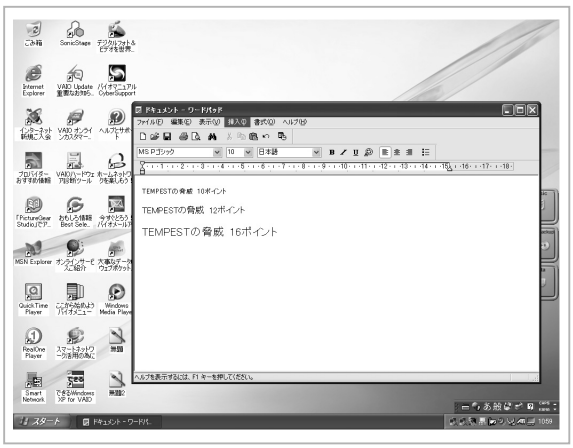

Fig.5 *Screen targeted for interception on the notebook*

4 Experimental results

4.1 Experimental equipment and interconnections

Table 4 summarizes the experiments described in this section, as well as the equipment and connections between various components. In the table, the plus symbol [+] indicates that the devices shown were used in combination. For example, “Desktop+LCD” indicates that the experiment was conducted on a video processor-equipped desktop computer connected to an LCD display.

Table 4 *Experimental equipment configurations*

	Desktop PC+LCD	Desktop PC+CRT	Note PC	Note PC+ CRT
Near magnetic field probe (section4.2)	Experiment A		Experiment B	
Antenna (section4.3)	Experiment C		Experiment D	
Injection probe (section4.4)	Experiment E	Experiment F	Experiment G	Experiment H

When desktops were targeted, the results of experiments using the antenna and near-magnetic field probe were nearly the same for the Desktop+LCD configuration as for the Desktop+CRT setup. Thus, the discussion of results here is limited to those for the Desktop+LCD configuration (experiments A and C). Furthermore, the experiments were conducted in an ordinary test room, not in an electromagnetically shielded environment such as an anechoic room.

4.2 Experiment using a near-magnetic field probe

Intercepting screen images requires an accurate grasp of the synchronous frequency of the video signals of the target equipment. Devices have unique synchronous frequencies, which are unrelated to the frequency bands of the relevant electromagnetic emissions. Thus, in this experiment, we verified the potential of obtaining the synchronous frequency by bringing the near-magnetic field probe into contact with equipment housings used as interception targets, as depicted in Fig.3.

The following section describes the experimental procedure and results with the ATI Radeon 9700 card (experiment A).

[Step 1]

Synchronous frequency is standardized by the Video Electronics Standards Association (VESA) according to screen width and number of colors [5]. In this experiment, the horizontal and vertical synchronous frequency of the interception targets was set at 64 kHz and 60 Hz, respectively. These synchronous frequencies were also set as initial values on the test receiver.

[Step 2]

To find the positions on the interception targets at which the electromagnetic emissions from the equipment housings were strongest, we brought the near-magnetic field probe into contact with the target equipment at various locations. As a result, we observed the following tendencies regarding the locations at which electromagnetic emissions were most apparent.

- Around the connectors on the body
- Around the connectors on the display side
- Around the display buttons and LCD bezel

The positions at which emissions are most apparent are indicated in Fig.6.

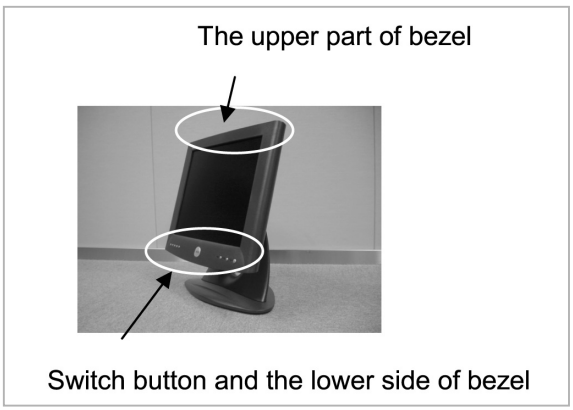

Fig.6 *LCD display positions at which strongest apparent electromagnetic emissions were observed (circled in white)*

[Step 3]

The intercepted screen was observed to find the reception frequencies most suitable for interception. At this stage, only the reception frequency was adjusted, not the synchronous frequency set in step 1. Computers generate electromagnetic waves in a variety of frequencies, so several reception frequencies are potentially suitable for screen interception. In our experiment, reception frequencies of 500 MHz to 1 GHz were often found suitable for screen interception using a near-magnetic field probe.

[Step 4]

Most of the reception frequencies of step 3 merely produced screens of video noise, as shown in Fig.7. However, particular reception frequencies yielded screens showing features of the screen images of the interception targets. In the case of the ATI Radeon 9700, this phenomenon appeared at around 530 MHz. As we approached the optimal reception frequency, we obtained a somewhat out-of-sync screen, as shown in Fig.8. The experimental equipment does not support reproduction of color information, so a monochrome screen

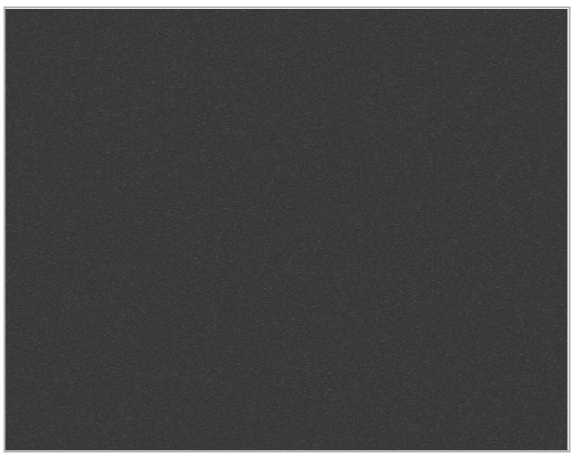

Fig.7 *Screen with video noise, before tuning*

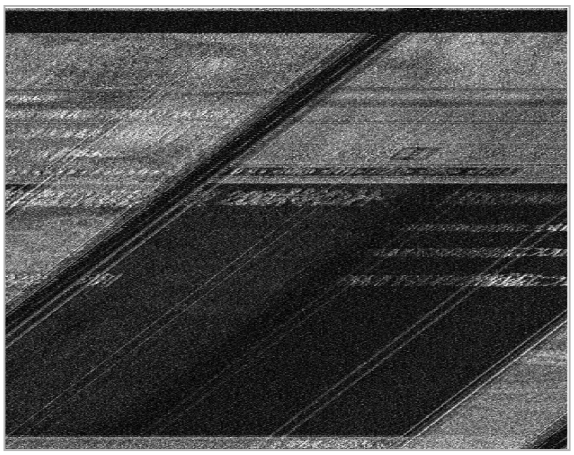

Fig.8 *Intercepted screen (unprocessed), after tuning*

was displayed even if the original screen was in color.

[Step 5]

As indicated in Fig.8, the screens obtained were not still images, but instead, moved vertically and horizontally. The horizontal and vertical synchronous frequencies were then adjusted to stabilize the image. The experimental equipment we used supported adjustment in increments of 10-6 kHz for the horizontal synchronous frequency and 10-6 Hz for the vertical synchronous frequency. At this point, we adjusted the reception frequency and searched for suitable contact positions for the probe. For a clearer picture, we also set up a method of averaging several frames of the intercepted screen. As a result, we were able to stabilize the intercepted screen as shown in Fig.9. Text in 10-point font or larger was legible on this intercepted screen. In Fig.9, the task bar on the bottom of a screen in Windows is visible above the black horizontal bands in the middle, and the clock at the far right was also legible.

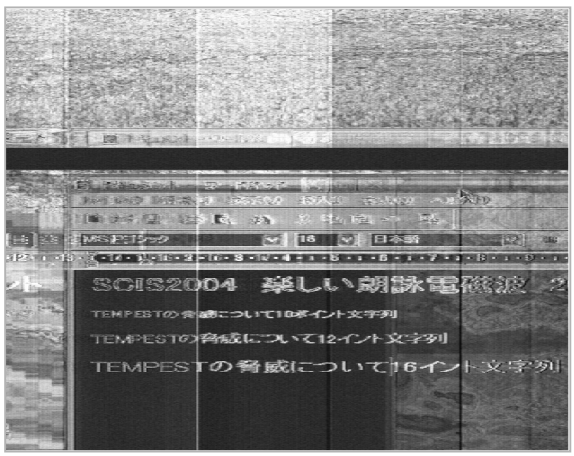

Fig.9 *Clearest screen intercepted in experiment A*

[Conclusion of Procedure]

The above procedure was repeated using the notebook computer (experiment B).

With the notebook, we observed the following tendencies regarding the positions at which electromagnetic emissions were most apparent.

- By the hinge above and to the left of the keyboard, when the LCD screen was open
- Around the left bezel of the LCD screen
- Behind the hinges and LCD screen
- Over the entire keyboard

The positions at which emissions were most apparent are indicated in Fig.10. The intercepted screen is shown in Fig.11.

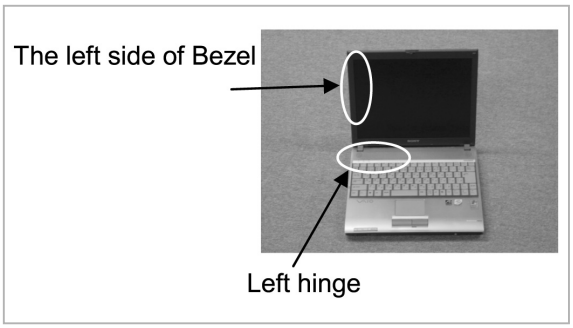

Fig.10 *Positions on the notebook at which strongest electromagnetic emissions were observed*

Fig.11 *Clearest screen intercepted in experiment B*

Synchronous frequencies are given in Table 5 for experiments A and B following both procedures. As shown in Table 5, there was slight variation in the measured synchronous frequencies, probably due to a lack of uniformity in the constituent parts and other factors. In any particular item of equipment, however, there was little fluctuation over time. The variation has no effect in regular use, but in screen interception based on electromagnetic emissions, changing the measured synchronous frequency by values in the hundredths of units upsets synchronization greatly, making the intercepted screen unrecognizable. This

means that extreme precision is required in matching synchronous frequency to intercept screens based on electromagnetic emissions. It also means that even in an environment with several computers running at once, it is possible to target one screen for interception based on its distinctive variation in synchronous frequency.

Table 5 *Synchronous frequency tuning results*

	Horizontal frequency [KHz]	Vertical frequency[Hz]
Radeon 9700	63.892403	59.9362
Geforce2	63.953513	60.012
Geforce3	63.99952	59.9944
Intel 82845	63.974302	60.04
VAIO V505	48.338321	59.973150

4.3 Experiment using an antenna

After a near-magnetic field probe is used to gain an accurate grasp of the synchronous frequency, it is easy to intercept free-space radiation with an antenna. Thus, we conducted a subsequent experiment to intercept desktop and notebook screens using free-space radiation (experiments C and D).

The experimental environment is shown in Fig.12. In experiment C, the ATI Radeon 9700 was used as the video card. The test receiver was adjusted to the obtained synchronous frequencies (horizontal: 63.892403 kHz; vertical: 59.9362 Hz), and screen interception was attempted with the antenna at a distance of 4 m from interception targets. For a clearer screen image, the frequency band for interception and the antenna orientation were adjusted while viewing the intercepted screen. An example of an intercepted screen is shown in Fig.13. In experiment C, reception frequencies suitable for interception were found at around 919.9 MHz. Text in nine-point font or larger was legible.

Experiment D was conducted similarly, but values were measured for the notebook. An example of a screen intercepted from 4 m away is shown in Fig.14. In experiment D, reception frequencies suitable for interception were found at around 844.8 MHz. Text in nine-point font or larger was legible. Figure 15 shows an example of a screen intercepted from a distance of 6 m in experiment D. Here, reception frequencies suitable for interception were found at around 989.4 MHz. Although text was hard to read, movement and changes on the screen were recognizable, such as when applications were launched or when screen savers were triggered. Thus, attackers would be able to make inferences as to user tasks.

Fig.12 *Experimental environment for interception using an antenna*

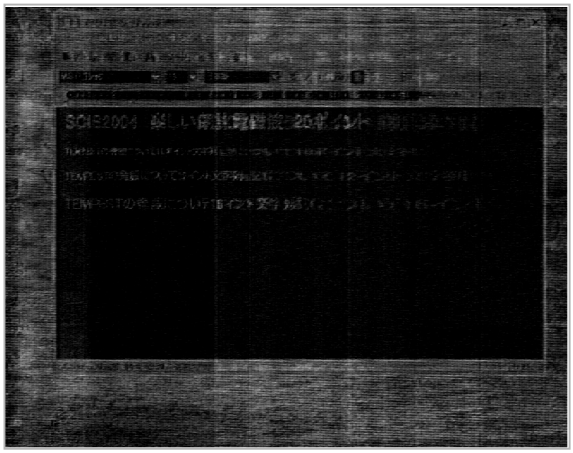

Fig.13 *Clearest screen intercepted in experiment C*

In this experiment, interception was possible whether the desktop display was a CRT or an LCD, and the reception frequencies were the same. Clearer screens were not necessarily obtained simply by aiming the antenna at the interception target. In many cases, receiving electromagnetic waves reflected from walls or other surfaces yielded a clearer screen. Thus,

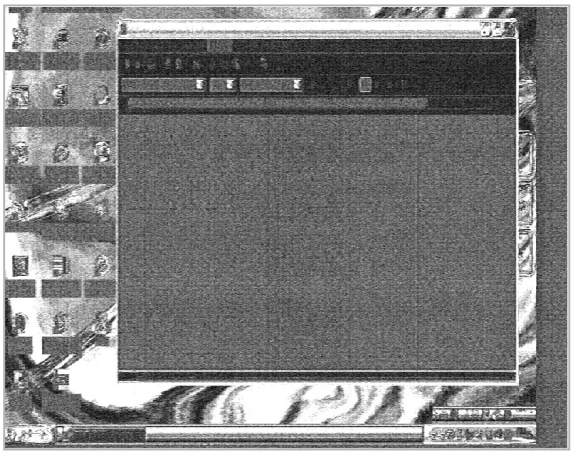

Fig.14 *Clearest screen intercepted in experiment D, at 4 m*

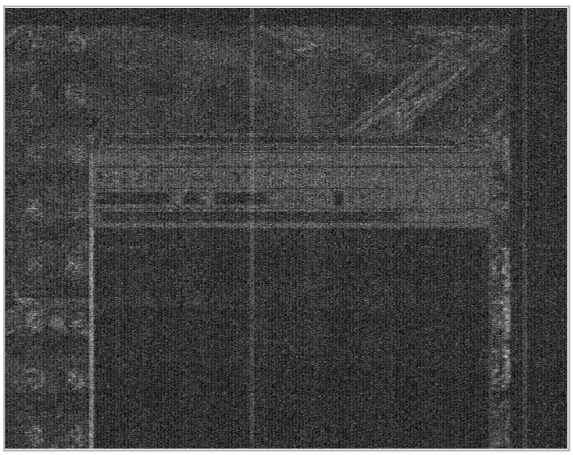

Fig.15 *Clearest screen intercepted in experiment D, at 6 m*

some trial and error is required in finding an antenna orientation suitable for interception.

Additionally, the intercepted screen was upset by the movement of people coming and going in the experimental environment. This was particularly noticeable when people came between the antenna and the interception target. For electromagnetic waves of 1 GHz and below, regulated by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI)[6], computers manufactured by Japanese companies were expected to feature fewer electromagnetic emissions. However, screens were intercepted by tuning to frequencies of 1 GHz and below as well. Thus, we must be careful even under current voluntary regulations, as screens can be intercepted even from trace electromagnetic waves. Furthermore, we confirmed that screens can be intercepted in the same manner at frequencies around 1.2 GHz as well.

4.4 Experiment using an injection probe

This section presents our experiment on intercepting emissions via power cable as the cable passes through an injection probe. Unlike free-space radiation, electromagnetic waves are easily conducted over cables, in which they are usually found at low frequencies. Thus, for the experiment in this section we targeted a low range of frequencies for interception, 30 MHz and below, in contrast to the high interception range targeted in the preceding experiments (i.e., 500 MHz and above).

When testing both LCD and CRT screens (experiments E and F, respectively) as the desktop output devices, interception was not clear in experiment E, but in experiment F, text in 20-point font or larger was faintly legible.

On the other hand, when targeting the notebook (experiment G), results varied depending on the position of the AC adapter. Two conditions can be imagined (conditions I and II) based on the position of the probe, as shown in Fig.16. Results indicated that interception was possible under condition II, but sometimes impossible under condition I. This may be a result of the properties of certain AC adapters that block emission of the screen signal through the process of converting alternating current to direct current within the adapter. These properties may have led to incompatibility between the adapter and injection probe.

We conducted an experiment taking into account likely use of typical notebooks, dis-

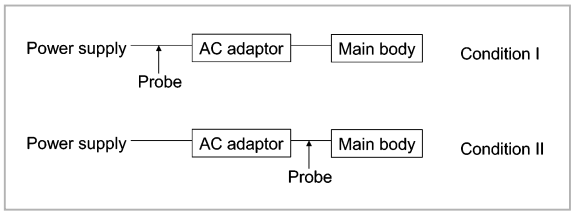

Fig.16 *Positions of the AC adapter and probe*

playing the screen output from the computer on a CRT (experiment H). The experimental environment in experiment H is shown in Fig.17. Here, a 30-m extension cord was used to supply power to the notebook and CRT, and the injection probe was fitted to the extension cord near the wall outlet. Results reflected those that would have been obtained if the probe had been used 30 m from the interception target. The intercepted screen is shown in Fig.18. The reception frequency was 23.8 MHz, and Fig. 18 shows the result of averaging for 128 frames. Text in 12-point font or larger was legible. It was also possible to discern movement and changes on the screen, as with screen savers and the like. Figure 19 shows an enlarged view of the lower-right portion of Fig.18. As the figure illustrates, text with easily recognizable features is legible, such as numbers or katakana characters. Note that although the extension cord is shown coiled in Fig.17, the intercepted screen was just as clear when the cord was unwound and extended.

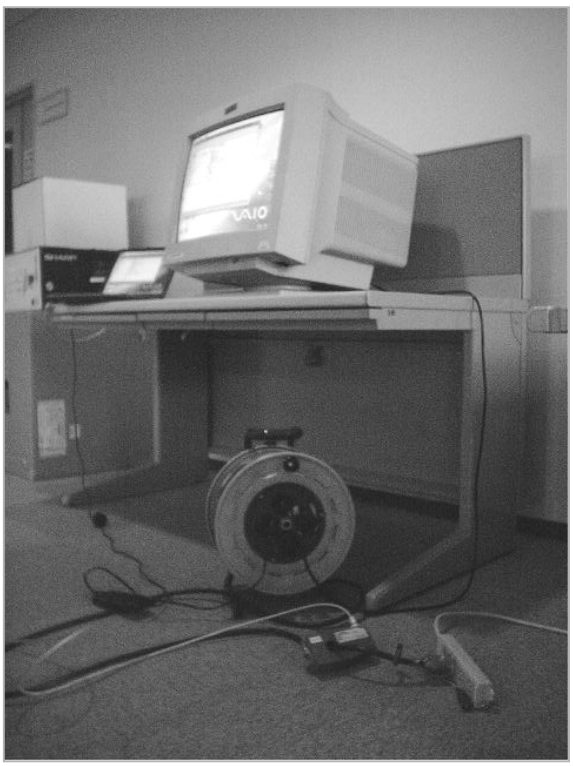

Fig.17 Environment of experiment H

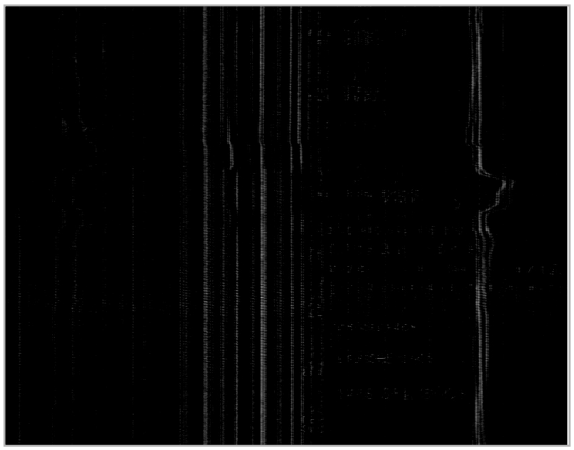

Fig.18 Clearest screen intercepted in experiment H

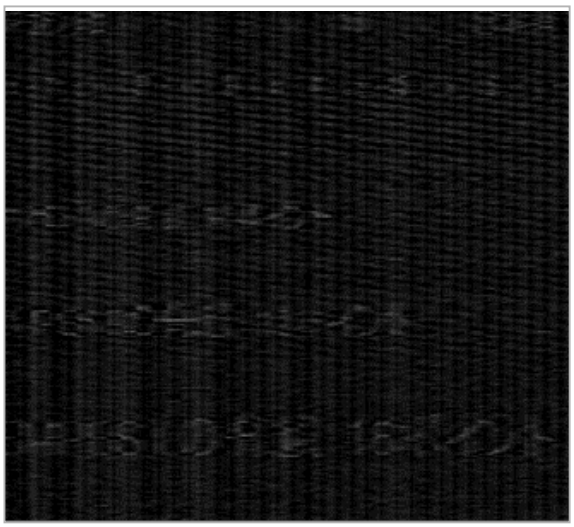

Fig.19 Screen of Fig.18, enlarged

5 Discussion

Based on the results of the experiments on screen interception from electromagnetic emissions presented in the preceding section, we have drawn the following conclusions regarding reception technology.

- Positions from which electromagnetic waves emanate vary depending on the housing material and shape of the target.
- Differences between CRT and LCD monitors do not affect the difficulty of interception.
- From the standpoint of interception difficulty, there is no difference between targeting desktops or notebooks.

The synchronous frequencies of video sig-

nals are standardized by VESA specification according to screen size and number of colors displayed. We determined the following with respect to this synchronous frequency value.

- Slight variation is seen compared with specification values.
- Variation in synchronous frequency is distinctive to particular items of equipment. This feature can be used to identify computers targeted for interception.

Furthermore, we have determined the following characteristics regarding electromagnetic waves targeted for interception.

- Even trace electromagnetic waves of 1 GHz and below, regulated under VCCI regulations, can be intercepted.
- Interception through power lines is possible.

However, the success or failure of interception through power lines tends to depend on issues such as compatibility between the adapter and probe when targeting notebooks or LCD monitors with an interposing AC adapter or similar device. For typical desktops and CRTs, interception is easy even at relatively far distances or with obstacles. Thus, these targets are easily susceptible to real threats.

Table 6 summarizes the relationship between relative difficulty and threat in each experiment. The ◎ symbol indicates that screens could be intercepted to reproduce text legible to most people without much difficulty. The ○ symbol indicates that screens could be intercepted to reproduce text that was legible to the experimenters. The × symbol indicates that text was not legible. In cases marked ○/×, different results were obtained depending on the relative position relationship between the AC adapter and probe, as shown in Fig.16. The – symbol indicates that no experiment was conducted. Notwithstanding these results it is difficult to evaluate objectively whether the text on intercepted screens is legible and can be interpreted. Context and prior knowledge are factors. The primary objective of presenting the specific experimental methods in this research was to enable third parties to reproduce the experiments. Thus, the results in Table 6 are limited to the subjective evaluations of the experimenters. In the future, it will be necessary to investigate objective evaluation methods, especially for experiments yielding results in the "○" category.

Table 6 *Relative difficulty and threat in each experiment*

	PC+LCD	PC+CRT	Note	Note+LCD	Note+CRT	Threat
Near magnetic field probe	◎	◎	◎	–	–	low
Antenna	◎	◎	◎	–	–	middle
Injection probe	×	○	○／×	○／×	○	high

As shown in Table 6, when an injection probe is used, interception is possible targeting fixed equipment such as ATM machines or electronic voting systems, so the threat is most pressing in these cases. Interception may be possible, for example, if the attacker has access to the same power transformer used for the target, even if the latter is in another room. Screen interception using an antenna also poses a threat, but the required size of the antenna depends on the reception frequency, so attackers in these cases may require larger devices. Reception is also susceptible to obstacles, which render interception difficult. If a near-magnetic field probe is used, it is easy to intercept clear screens; however, the probe must in this case be in contact with the target equipment. It is thus hard to imagine as a realistic threat. Thus, we may conclude that the level of real threat posed is inversely proportional to the clarity of the screens obtained. In any case, we have shown that screen interception is possible with current technology, and we can conclude that with progress in technology in electromagnetic-wave reception and advances in image processing, it will be critical to develop countermeasures against screen interception from electromagnetic emissions.

6 Conclusions

This paper presents, in greater detail than

seen in previous reports, specific experimental equipment, procedures, and results relating to the potential for intercepting computer screen images through electromagnetic emissions. We found that the success of screen interception varies depending on the experimental environment, including the various devices involved. Thus, this paper is limited to qualitative evaluations for a few interception targets. We nevertheless hope that this paper will serve as a significant resource in its presentation of an experimental outline that is sufficiently specific to enable others to reproduce these experiments, and we would be pleased if the results of this paper can contribute to the development of research on policies to deal with interception of electromagnetic emissions.

References

1 J.J.Quisquater and F.Koeune, "Side Channel Attacks", CRYPTREC Report 1047, 2002. (available at http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf)

2 S.Micali and L.Reyzin, "Physically observable cryptography", Theory of Cryptography Conference 2004 (TCC2004), Lecture Notes in Computer Science, Vol.2951 Springer-Verlag, pp.278-296, 2004.

3 IST(Information Security Technology Study Group) report 2002.

4 Anritsu products catalog 2004.

5 http://www.vesa.org/, 2004.

6 http://www.vcci.or.jp/, 2004.

***TANAKA Hidema**, Ph.D.*

Researcher, Security Fundamentals Group, Information and Network System Department

Cryptology, Information security

***TAKIZAWA Osamu**, Ph.D.*

Senior Researcher, Security Advancement Group, Information and Network Systems Department

Contents Security, Telecommunication Technology for Disaster Relief

***YAMAMURA Akihiro**, Ph.D.*

Group Leader, Security Fundamentals Group, Information and Networks Systems Department

Information security, Cryptography, Algebraic systems and their algorithms