A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation

Yuichi Hayashi
Tohoku University
Aramaki aza Aoba 6-3-09,
Aoba-ku Sendai, Japan
+81-22-795-6094
yu-ichi@gcc.ne.jp

Naofumi Homma
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
homma@aoki.ecei.tohoku.ac.jp

Mamoru Miura
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
miura@aoki.ecei.tohoku.ac.jp

Takafumi Aoki
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
aoki@ecei.tohoku.ac.jp

Hideaki Sone
Tohoku University
Aramaki aza Aoba 6-3,
Aoba-ku Sendai, Japan
+81-22-795-6091
sone@isc.tohoku.ac.jp

ABSTRACT

The use of tablet PCs is spreading rapidly, and accordingly users browsing and inputting personal information in public spaces can often be seen by third parties. Unlike conventional mobile phones and notebook PCs equipped with distinct input devices (e.g., keyboards), tablet PCs have touchscreen keyboards for data input. Such integration of display and input device increases the potential for harm when the display is captured by malicious attackers. This paper presents the description of reconstructing tablet PC displays via measurement of electromagnetic (EM) emanation. In conventional studies, such EM display capture has been achieved by using non-portable setups. Those studies also assumed that a large amount of time was available in advance of capture to obtain the electrical parameters of the target display. In contrast, this paper demonstrates that such EM display capture is feasible in real time by a setup that fits in an attaché case. The screen image reconstruction is achieved by performing a prior course profiling and a complementary signal processing instead of the conventional fine parameter tuning. Such complementary processing can eliminate the differences of leakage parameters among individuals and therefore correct the distortions of images. The attack distance, 2 m, makes this method a practical threat to general tablet PCs in public places. This paper discusses possible attack scenarios based on the setup described above. In addition, we describe a mechanism of EM emanation from tablet PCs and a countermeasure against such EM display capture.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection—Physical security

General Terms

Security

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
Copyright © 2014 ACM 978-1-4503-2957-6/14/11...\$15.00.
<http://dx.doi.org/10.1145/2660267.2660292>.

Keywords

Touch-screen devices; Tablet PCs; Remote screen-image visualization; EM information leakage

1. INTRODUCTION

The number of touchscreen devices such as tablet PCs has rapidly increased in recent years. Accordingly, many users of such devices enjoy browsing and inputting personal information in public spaces, where third parties are present, in addition to doing so in private spaces. Unlike conventional PCs, the users of tablet PCs usually input data with keyboards displayed on the screen, using so-called software keyboards, as shown in Fig. 1.

Such integration of display with input device causes a serious risk of harm when the integrated display is captured by malicious attackers. Both the entered keys and their purpose (i.e., place on the screen), displayed on the same screen, can be stolen simultaneously by a single display capture. In particular, software key-boards often enhance the entered key by luminance changing or visually popping-up to support user confirmation, which makes it easier to steal key information. Even if an entered key is changed to an asterisk in the password section, as shown in Fig. 1, an attacker can obtain the key information from the enhancement effects. Such threats are potentially present in many applications that use login

Figure 1: Typical screen shot of tablet PC with software keyboard.

information (e.g., e-mails, schedulers, SNS services, online banking) or authentication information (e.g., online payments, and security codes in credit card services).

The problem of information leakage through electromagnetic (EM) emanation has been studied in the field of electromagnetic compatibility (EMC) research. Such research is often referred to as TEMPEST, a codename referring to techniques and standards to suppress emissions that might compromise security. In the context of TEMPEST research, EM emissions from information and communications technology (ICT) devices are defined as “unintentional intelligence-bearing signals” which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment [1]. The topics of TEMPEST include technologies for suppressing such unnecessary signals from ICT devices, studies investigating EM emanation, and so forth. In its early stages, technology for performing TEMPEST attacks required expensive and scarcely available equipment for monitoring such EM emanations, and the security community previously believed that such highly sophisticated monitoring was possible in only military- and government-level attacks.

At present, ICT devices at risk for EM information leakage include many commercial products, such as CRT and LCD monitors [2]–[12], printers [13], and keyboards [14][15]. In particular, the threat of display capture via EM emanation, called EM display stealing, has been studied for the relatively larger displays of desktop and notebook PCs. More precisely, the possibility for and limitations of EM display stealing have been discussed for an individual display attached to a PC owned by a specific user and with assuming that leakage parameters specified to the individual can be determined in advance given sufficient time. In addition, the conventional setups for EM display stealing were non-portable and assumed to be placed in doors or cars, which imposed a limit on proximity of approach to the target display. Therefore, the previous studies [6][8][11] have discussed mainly zone-based countermeasures [16] that decrease the intensity of EM emanations to the background noise floor before those emanations reach eavesdroppers. Figure 2 depicts the concept of a zone-based countermeasure.

EM display stealing from tablet PCs looks difficult in the context of conventional studies because tablet PCs have weaker EM emissions than conventional PCs do. Such weaker EM emissions are reduced to the noise floor quite close to the devices. In addition, tablet PCs are often manipulated by moving. This usage makes time-intensive parameter tuning much more difficult. For the above reasons, the threat of EM display stealing from tablet PCs has not been discussed in conventional studies.

Through this paper, we present an emerging and practical threat to tablet PCs in public spaces. We assume here that attacks must be conducted very close to target tablet PCs. This assumption requires a small eavesdropping setup that can be easily carried by the attacker and a real-time identification of the leakage parameters. Specifically, the contributions of this paper are as follows.

–Portable and real-time stealing setup: A portable stealing setup is constructed to observe EM radiation corresponding to screen images and input keys near tablet PCs. Filling the functional insufficiency by profiling and signal processing techniques, the portable setup can perform a real-time EM display stealing comparable to conventional non-portable setups. In particular, we apply a prior course profiling to a target and derive an accurate image by signal processing, which makes the system robust to individual difference, eliminates the time for estimating leakage

Figure 2: Concept of zoning-based countermeasure against EM display stealing [16].

parameters, and enables to steal information immediately by loading the leakage parameter.

–Demonstration using actual tablet PCs: The demonstration of the above EM display stealing is performed with widespread tablet PCs. As a result, an entered key and its position are clearly stolen from a tablet PC 2 m away from the setup. Moreover, possible attack scenarios are derived from the experimental results.

–Leakage mechanism and countermeasure: A mechanism of EM emanation from tablet PCs is discussed. Using an EM interference (EMI) model, we present how EM information leakage can be caused even by an unintentional antenna structured from internal wires. In addition, a cost-effective and post-production countermeasure against such EM display stealing is discussed.

2. EM DISPLAY STEALING FROM TABLET PCS

2.1 Basic concept

This section describes a concept for EM display stealing from tablet PCs by use of a portable setup with prior profiling and real-time signal processing techniques. A conventional setup for EM display stealing is composed of a receiver to capture EM emanations, a device to measure the received EM trace, and a display. In particular, the measurement device requires a wide resolution bandwidth (RBW) and a significant sampling rate [6][11][12]. As a candidate to replace these devices, software-defined radio devices equipped with a high-speed analog-to-digital converter have become available inexpensively in recent years. Such devices can program any signal processing technique for digitized data. Though the sampling rate is limited to at most 100 MSa/s, an RBW of 50 MHz is comparative to that of a conventional device. In addition, the signal processing can adapt the size of images reconstructed from EM emanations according to the available display. Thus, a software-defined radio device can replace the measuring device, which significantly increases the portability of the setup.

Another drawback of the conventional display stealing method is that it requires a large amount of time to tune the electrical parameters (i.e., leakage frequency, horizontal scan frequency, and vertical scan frequency). This is because such parameters are unique to the individual hardware units, even among ostensibly identical devices [7][17]. Moreover, the reconstruction of leaked images has conventionally been carried out by inputting the tuned horizontal and vertical synchronization frequencies directly into a monitor. It was therefore necessary to measure the synchronization signals with a very high precision. For example, the conventional methods would require finding an exact value of 73.11696 kHz for the horizontal synchronization frequency. When inaccurate horizontal and vertical scan frequencies are obtained, each reconstructed image has a different distortion, resulting in the reduction of visibility. Here, we exploit prior profiling and real-time signal processing to reconstruct the distorted images.

Figure 3 shows an overview of the EM display stealing, where the receiver (i.e., an antenna) and the display are omitted. In the profiling phase, we first study the three electrical parameters of a target tablet PC and acquire a reference screen image with a software keyboard, as shown in Fig. 4. The assumption here is that possible differences in parameter values among the same model (i.e., the same product) are adjustable by the following processing. We then receive the EM emanations and demodulate them by the amplitude of the leakage frequency from the advance profile. The demodulated (analog) signals are sampled at an equivalent time interval and converted to digital signals. The obtained digital signals are replicated by a number of samples, determined by the profiled parameters and the sampling rate of the device. Note that through the preliminary experiment, we confirmed pixels data were leaked sequentially from tablet PCs. We then reconstructed a display image by separating the leaked pixels data at a specific timing corresponding to the display resolution, in the equivalent manner as in CRT. In this paper, we call the separation periods in horizontal direction and vertical direction "horizontal scan frequency" and "vertical scan frequency", respectively. After the replication, we obtain a series of 2D images from the observed EM emanations (Fig. 3(2)).

The reconstructed 2D images include a skew (i.e., shear or change in shape from rectangle to parallelogram) and a kind of translational displacement. Skew occurs when the original horizontal scan frequency is not equal to an integer multiple of the sampling rate of the device. (In this sense, the distortion is not actually a skew, but we approximate it as a skew for the simplicity of the subsequent signal processing.) Skew is not a concern in the conventional setup because of the very high sampling rate. In contrast, translational displacement always happens because the initial point for drawing an image is not obtained from the measured data (Fig. 3(3)). Moreover, the proposed method shown in Figure 3(3) does not require a high-precision synchronization signal from the beginning because, even if a relatively low-precision signal is acquired, the screen is recovered by using an image acquired in advance from the tablet. In the case of the tablet used in this paper, the frequency value to two decimal places (i.e., 73.12 kHz instead of 73.11696 kHz) is sufficient for the horizontal synchronization frequency. As a result, we can measure such horizontal synchronization frequency immediately. Furthermore, the conventional methods have difficulty in reconstructing screens that exceed the resolution of the monitor used to reproduce the target screen while the proposed method has no limit on the screen resolution since the images are reconstructed by signal processing on a computer.

Figure 3: Concept of EM display stealing for tablet PCs by portable setup.

Figure 4: Profiled image.

The visibility of 2D images is greatly diminished by the above distortions. In particular, the distortion by the translational displacement is different for each frame, which makes it difficult to recognize entered keys. However, the above distortions can be corrected by the following signal processing technique. In addition, after correction, automatic keystroke detection can also be performed by a simple signal processing on two frames, those before and after entering a key.

2.2 Visibility improvement and keystroke detection

2.2.1 Skew correction

Skew transformation of the reconstructed image can be corrected on the basis of the Fourier amplitude spectrum of the image.

Consider an $N_1 \times N_2$ -pixel image $x(n_1, n_2)$. Let $X(k_1, k_2)$ denote the discrete Fourier transform of the image. $X(k_1, k_2)$ is given by

$$X(k_1, k_2) = \sum_{n_1, n_2} x(n_1, n_2) W_{N_1}^{k_1 n_1} W_{N_2}^{k_2 n_2},$$

where $W_{N_1}^{k_1 n_1} = e^{-j\frac{2\pi}{N_1} k_1 n_1}$ and $W_{N_2}^{k_2 n_2} = e^{-j\frac{2\pi}{N_2} k_2 n_2}$. The amplitude spectrum $A(k_1, k_2)$ is given by $A(k_1, k_2) = |X(k_1, k_2)|$. When a software keyboard exists in the reconstructed image, significant magnitude is observed along a direction in the frequency image (i.e., the amplitude spectrum), which is perpendicular to the edge of each key in the spatial image. Since this relation remains unchanged even when the keys are slanted by the skew of the image, the skew can be estimated by the dominant direction in the amplitude spectrum. To determine the direction, we can use any line detection method. In this paper, we employ the Standard Hough Transform, a commonly used method of detecting straight lines [18]. When a line $\rho = k_1 \cos \phi + k_2 \sin \phi$ is detected in the amplitude spectrum $A(k_1, k_2)$, the homography matrix for correcting the skew of the image $x(n_1, n_2)$ is given by the following equation:

$$H_{\text{skew}} = \begin{bmatrix} 1 & \tan(\phi + \frac{\pi}{2}) & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

2.2.2 Translation correction

Translational displacement of the reconstructed image can be corrected by an image-matching method with a screenshot of the target display taken in advance (during the profiling phase). A cross-correlation function is computed between a reconstructed image and the screenshot. Because the peak of this function corresponds to the translational displacement between the two images, computing the correlation function makes it possible to estimate and correct the translational displacement. Note that shape information, such as edges, is preserved between the captured display and the reconstructed image, but brightness information is not preserved. For this reason, a Sobel filter [19], which detects edges in images, is applied to each image before computing the correlation function.

Consider a skew-corrected image $x'(n_1, n_2)$ and a screenshot image $y(n_1, n_2)$. Let $x'_e(n_1, n_2)$ and $y_e(n_1, n_2)$ denote the edge images originating from the two images, respectively. The cross-correlation function between them is defined by

$$r(n_1, n_2) = \sum_{\xi, \eta} x'_e(\xi - n_1, \eta - n_2) y_e(\xi, \eta).$$

When the peak of the correlation function is $(n_1, n_2) = (\alpha, \beta)$, the homography matrix for correcting the translational displacement of $x'(n_1, n_2)$ is given by

$$H_{\text{trans}} = \begin{bmatrix} 1 & 0 & -\alpha \\ 0 & 1 & -\beta \\ 0 & 0 & 1 \end{bmatrix}.$$

2.2.3 Keystroke detection

After skew transformation and translational displacement are corrected in each frame, keystrokes in the sequence of reconstructed images can be detected by the difference between neighboring (i.e., temporally adjacent) frames. Software keyboards usually highlight key inputs by popping up keys or by reversing the

Figure 5: Block diagram and photos of portable setup for EM display stealing.

Figure 6: Block diagram of profiling setup.

key luminance to support user confirmation. We focus on this feature to detect key inputs from the sequence. In the following, we describe an algorithm for detecting keystrokes when the luminance of the pressed key region is reversed. We note here that similar techniques can be used in other cases, such as when a pressed key visually pops up.

Figure 7: Skew correction.

Figure 8: Keystroke detection.

For each frame of the sequence, a difference image is found by subtracting the previous frame. When keys are pressed, high-intensity regions are observed in the difference image, which is caused by reversing the pressed key luminance. The pressed keys are identified by matching between the regions and the profiled screenshot (i.e., the keyboard layout). In this paper, the luminance values are associated with the scan codes of keys. The correspondence between them is denoted by a function s , such as $s('a') = 65$.

Consider a difference image $d(n_1, n_2)$ and a keyboard layout image $l(n_1, n_2)$. A masked difference image is defined by

$$l'(n_1, n_2) = \begin{cases} l(n_1, n_2) & \text{if } d(n_1, n_2) > 0 \\ 0 & \text{otherwise} \end{cases}$$

For an arbitrary key c , let $|s(c)|$ be the number of pixels satisfying $l'(n_1, n_2) = s(c)$; that is, the number of pixels varying between neighboring frames. When $|s(c)| \geq \tau$, the key c was pressed. In this paper, we assume $\tau = |s(c)| + 3\sigma$, where $|s(c)|$ is the mean of $|s(c)|$ and σ is the standard deviation for all keys of c .

Using the above keystroke detection, eavesdroppers can obtain personal information, such as passwords, even when the information is entered too quickly to be recognized by human eyes.

3. EXPERIMENTS

This section demonstrates the feasibility of applying the above EM display stealing to popular tablet PCs.

3.1 Experimental setup

Figure 5 shows a block diagram and photos of the EM display stealing setup in this experiment. The measurement device was implemented by a compact software-defined radio device (USRP N210). The receiver employs the superheterodyne system, which converts a received signal to a fixed intermediate frequency (IF),

amplifies the IF signal by an intermediate amplifier, and demodulates the result to detect the original information. The detected signal is converted into a digital signal. The IP packet containing the signal is then transferred to a PC via Ethernet for follow-up signal processing. In the experiment, the PC and the radio device were connected by a wired IP-based network. Note here that we could connect them wirelessly and use a remotely located computational device. The receiver was implemented by an off-the-shelf UHF antenna (YAGI UwPA), where the reception frequency is from 470 MHz to 710 MHz and the antenna gain is from 4 dB to 5 dB. All the components of the setup are stored in an attaché case, as shown in the bottom of Fig. 5, that is compact and light for easy carrying.

Figure 6 depicts a setup for profiling leakage frequency, horizontal scan frequency, and vertical scan frequency. The leakage frequency is identified by scanning frequencies beginning with initial horizontal and vertical scan frequencies that depend on the display specification. The EM scanner is employed to fix and manipulate a magnetic field probe over possible measurement points. Once the leakage frequency is fixed, the horizontal and vertical scan frequencies are fine-tuned for accuracy of hertz by monitoring reconstructed images on a high-resolution display. We can identify the above three frequencies in a short time by using the setup in Fig. 6. Note here that the profiling procedure is also possible with the portable setup in Fig. 5 if we have a longer identification time. As a result, we identified a leakage frequency of 653 MHz, a horizontal scan frequency of 73.12 kHz, and a vertical scan frequency of 59.95 Hz in this experiment. The target tablet is one of the most widespread tablets, with a 1920×1200 display and total sales in the tens of millions of devices.

3.2 Image correction and keystroke detection

This section presents the first experiment for the image correction processing described in Section 2. In this experiment, we

observed EM emanations from the target tablet with the setup shown in Fig. 5, where the leakage parameters identified above were used for the reconstruction. We then demodulated the EM emanation by amplitude and converted it into the corresponding digital signals. The obtained digital signals were replicated by a number of samples determined by the profiled horizontal scan frequency and the sampling rate of the device. After the replication, we obtained a series of 2D images from the observed EM emanations.

Figure 7 (a) shows an example of the originally reconstructed image, where a kind of skew transformation is observed. This is because the sampling rate of the software-defined radio device is not an integer multiple of the horizontal scan frequency of the device, and therefore the demodulated signal is folded to the 2D digital image incorrectly. To correct the skew transformation, the amplitude spectrum of the image is calculated as shown in Figure 7 (b). In the amplitude spectrum, a dominant direction indicating the skew parameter can be determined by a line detection method (here, Hough transformation). Figure 7 (c) shows the result after skew correction. We then calculate the cross-correlation function between the skew-corrected image and a screenshot image of the target display. Figure 8 (a) shows the image after translational displacement has been corrected. In addition, we detected keystrokes from the difference among neighbor frames in the reconstructed image sequence. Figure 8 shows an example of keystroke detection, where the input 'r' key was detected by the difference image (Fig. 8 (c)) between a frame without the key input (Fig. 8 (a)) and a frame with the key input (Fig. 8 (b)).

3.3 Evaluation of individual difference in the same model

This section demonstrates, through the second experiment, that individual differences among devices of the same model are negligible and thus a set of profiled frequencies is applicable to other individuals in the same model.

Using the setup in Fig. 5, we evaluated the visibilities of images reconstructed from EM emanations of five devices of the same model. The display surface of tablet PCs faced the receiver from 30 cm away. For all five devices, we used the same parameters as profiled in advance in the manner described above. The experiments were conducted in a common laboratory space where other PCs and electronic devices, such as LCD displays, were operating near the experimental setup. The five devices were purchased from different stores at different times. The production lot numbers differed between devices.

Figure 9 shows the reconstructed images, where each individual has two images, with and without a key input. We note here that all images were obtained in real time. We confirmed that all five displays were clearly reconstructed by the same parameters, although the contrasts were slightly different from each other. In addition, we can clearly identify which key is pressed. Automatic keystroke detection was also possible for all images.

3.4 Evaluation at different measurement distances

This section shows the third experiment, which evaluates possible distances for EM display stealing. The experiment was conducted with the setup in Fig. 5 at the same laboratory space described in the above section. Device No. 5 from the above experiment was used as the target device. Assuming that the tablet would be used in a public space, we evaluated the visibilities of reconstructed images for different distances between the setup and the tablet, ranging from 10 cm to 2 m.

Figure 9: Reconstructed images for different individuals.

Figure 10: Reconstructed images for different distances.

Figure 11: EM Intensities at different distances.

Figure 10 shows the images reconstructed from EM emanations where the antenna was placed 10, 50, 100, 150, and 200 cm away from the target. Each distance has two images, with and without a key input. The results indicate that all the images are successfully reconstructed and visible. As in the above experiment, we can clearly distinguish the key input from the two images. We note that all of these images were captured in real time. Any additional filtering and averaging procedures were performed on the images. The images reconstructed by EM emanations 2 m away from the tablet were the most obscure in the experiment. However, we confirmed that the difference image between a frame with and a frame without a key input clearly enhanced the key input, as shown in Fig. 8.

Figure 11 displays the intensity of EM emanations at different distances, where the vertical axis indicates the signal intensity observed at the software-defined radio device and the intensity value is normalized by the intensity at 10 cm. It is difficult to formalize the resulting intensities because there are many other electronic devices around the experimental setup and the emanation source might not be approximated by a reduction model of near EM fields based on an ideal antenna structure. However, we can estimate the boundary of near and far EM fields from the results, where the intensity fell exponentially up to 50 cm comparable to the wavelength of the leakage frequency, and then reduced linearly from greater distances. In other words, the near EM field was observed up to 50 cm and the far EM field was observed from greater distances. This result suggests that the maximum distance could be extended by optimization of the antenna (e.g., the use of a high-gain antenna).

3.5 Discussion of possible attacks

The above results indicate that EM display stealing for tablet PCs becomes a possible threat with use of a portable setup and the associated profiling and signal processing. Due to the portability of the setup, eavesdroppers can access a target tablet used in public spaces before the weak EM emanations are reduced to background noise. In addition, by using the profiling and signal processing, we can apply the technique to any tablet PC that is profiled in advance.

Figure 12 shows images of some typical scenarios in which EM display stealing can be conducted in public spaces (e.g., in a café or on transportation). Eavesdroppers can perform such EM display stealing on any tablet PC used near the setup if the product model is included in the list of profiled models. We usually permit other people to be within a distance of 2 m in many scenarios. Such

Figure 12: Typical scenes of EM display stealing by portable setup.

Figure 13: Reconstructed images of other products.

(a) Front side.

(b) Back side.

Figure 14: EM field distribution of leakage frequency on tablet surface.

Figure 15: Visibility of reconstructed images for different angles.

expansion of applications is the major difference from the conventional setup.

In addition, we can connect the output of the setup to a smartphone or a tablet through a remote desktop, which means that eavesdroppers can manually confirm reconstructed images in real time. Such instant confirmation makes it possible to improve the visibility of reconstructed image and select only valuable images.

Figure 13 shows the reconstructed images for other four products (three different tablet PC models and one smartphone), where the EM emanations were received by the same setup at a distance of 10 cm. We can confirm that all the key arrangements are visible. Though some visibilities look lower than those of the above product, we can improve them by adjusting the characteristics of the antenna according to the leakage frequency. In contrast, if eavesdroppers identify the product to be attacked in advance, they can optimize their setup according to profile results. Moreover, an optimized antenna makes the maximum stealing distance much longer. Thus, the result suggests that the EM display stealing by our setup can be applied to other touchscreen devices.

4. DISCUSSION OF LEAKAGE MECHANISM

Figure 14 shows the EM field distribution of the leakage frequency (653 MHz) on the front and back surfaces of the tablet. The EM field distribution was measured by the EMC Scanner shown in Fig. 6. The measurement interval was 5 mm, which is sufficiently smaller than the wavelength of the measured frequency. The total number of measurement points was about 1600 points, and at each of them, the EM field was measured by the Max-Hold function of the spectrum analyzer. In this measurement, we averaged 10 obtained signals to suppress the influence of background noise. In addition, we subtracted the EM radiation with turning off the display from turning on the display. The radiation map suggests that the EM field of 653 MHz was concentrated on the left half-region of the display at the front surface (Fig. 14 (a)). In contrast, on the back side, the distribution of the EM field is not concentrated (Fig. 14 (b)). Moreover, a continuous distribution along the edge is observed for the front side, but the electromagnetic field distribution of the leakage frequency is discrete for the back side.

Figure 15 indicates the visibilities of reconstructed images for different angles to the setup, where the setup is located 50 cm away from the tablet. A clear image was obtained when the tablet front surface directly faced the antenna (0°). At angles of 180° and 270°,

Figure 16: EM intensities for different angles.

Figure 17: Disassembled tablet PC.

Figure 18: Reconstructed images from EM radiation at the points in Fig. 17.

the contrasts were decreased but the keystrokes were still successfully identified. However, the image at an angle of 90° was invisible. Figure 16 shows the signal intensity for the four angles, where the values are normalized by that at 0° . The results clearly show that the strongest emission occurs from the tablet's front surface.

We then disassembled the tablet and reconstructed the screen image by measuring EM radiation emitted from some points on the device interior, in order to conduct a more detailed investigation regarding the points where strong emissions were observed in the magnetic field distribution on the front surface of the tablet (i.e., FPoints 1-5 in Fig. 14). Figure 17 shows the internal structure of the disassembled tablet, where BPoints 1-6 correspond to FPoints 1-6 on the front surface, respectively. BPoint 7 indicates another point on the center of the screen, and BPoint 8 indicates the cable (LVDS/FPD-Link) connected to the display. With the disassembly, we found that the parts where strong EM radiations were observed on the front surface corresponded to the metallic edge parts enclosing the display. For measuring the EM radiation, we replaced the antenna part of the setup shown in Fig. 5 by a near field probe (LANGER Near Field Probe RF R 400-1) and used the EM radiation emitted from BPoints on the device interior. We then reconstructed the screen image by the EM radiation measured at the BPoints.

Figure 18 shows the results of images reconstructed by the EM radiation from BPoints 1-5, and 8. Note that due to the lower gain of the near field probe, the measured EM field strength is lower. For this reason, the reconstructed image is dimmer than the images in the previous figures. Although there are differences in screen brightness, we verified that the screen can be reconstructed at the points where strong emissions were measured at the leakage frequency. Since the components other than edge consist of conductors, we also reconstructed the screen by measuring the emitted EM radiation at BPoints 6 and 7 as well, as shown in Fig. 17. The results are shown in Fig. 19. We found that the screen images cannot be reconstructed by the emitted EM radiation at these points. Similarly, it was difficult to reconstruct the screen image from EM radiations at the other locations on the back of the display. The same results were also obtained for the case of the front-side of the display. Figure 20 shows the images reconstructed with the EM radiations of FPoint2 (at the edge) and FPoint6 (at the center of the screen). The result suggests that the leakage from the tablet PC used in the measurement was likely caused by the edge of the display acting as an antenna.

We also used a near field probe to scan the interior of the tablet PC in order to identify the source of the screen information leakage. As a result, we found that the component where the clearest reconstructed image was measured at the leakage frequency was the flat cable connected to the display (BPoint 8) as shown in Fig. 17. We consider that above-mentioned leakage is caused by digital signals driving the screen through the cable. This result is in fair agreement with that of previous study [5].

Based on the above results, we discuss how the strong EM emission is generated from the front surface. We confirm from Fig. 14 (a) that the EM field of the leakage frequency (653 MHz) is distributed along the edge of the front screen. The wavelength of the leakage frequency is almost 45 cm, which corresponds to the length of the screen edge. From that fact, we consider the leakage frequency of 653 MHz, which would be one of the harmonics of a frequency driving the display, and attribute this to propagation through the wiring pattern on a printed circuit board or

Figure 19: Reconstructed images from EM radiation at the center of the screen in Fig.17.

Figure 20: Reconstructed images from EM radiation at the points on the display (Fig.14(a)).

Figure 21: EM field distribution of leakage frequency on tablet surface (Other product 4).

Figure 22: Model of information leakage from tablet PC via EM field.

(a) "SANTE" EMI shielding films.

(b) Applying countermeasure to tablet PC.

Figure 23: Countermeasure based on EM shielding film.

Figure 24: Reconstructed images with and without countermeasure.

communication cables and emits through an antenna constructed by the wiring patterns and cabling.

To check whether the above consideration can be applied to other devices as well, we measured the leakage frequency distribution on another tablet PCs with a different size. The results are shown in Fig. 21. The leakage frequency for this device was 714 MHz and the wavelength was about 42 cm. At the leakage frequency, the length of the parts where the EM radiations were strongest was about a single wavelength of the leakage frequency, which is the same as in the case of Fig. 14(a). The result backs up the above consideration.

Figure 22 illustrates the concept of a radiation model of EMI [20–23] for such emissions. The digital signals in the device, which include the driving signal of the display, are represented as a source signal and shown in Fig. 22 (a). According to the signal's peaks and valleys, the spectrum is spread over a wide band, as shown in Fig. 22 (b). If the significant frequency components match the frequency characteristics of the antenna constructed by the wiring patterns and physical structure of the substrate (Fig. 22 (c)), the EM wave is radiated efficiently, as shown in Fig. 22 (d),(e).

In actual devices, some physical structures behave as an antenna due to coupling capacitance, induction between wires, and high-frequency components contained in the rising and falling edges of

the signal. As a result, strong EM radiation occurs from the antenna. Thus, EM radiation is generated through such unintentional antennas in low-power-consumption devices, such as tablet PCs, in comparison with desktops and notebook PCs. The above radiation would make it possible to observe the leakage information at about 2 m away from the device.

5. A COUNTERMEASURE

This section discusses a countermeasure to prevent EM display stealing from tablet PCs. From Figs. 14 and 16, we observe that the leakage EM waves were mainly radiated from the front side of the display. In this section, we focus on an EM-shield-based countermeasure that can be applied after device assembly.

In general, such EM shielding is a good practice to reduce the EM field in a space by using barriers made of conductive or magnetic materials. Shielding is typically applied to enclosures to isolate electrical devices from the 'outside world,' and the barrier is preferably composed without any additional space to increase the shielding effect. Note, however, that if the shield covers the full display surface, the usability of the screen is reduced significantly. Addressing the above difficulty, we discuss a technique for suppressing EM radiation without reducing the usability of the screen by using a shielding material made of a conductive mesh.

As an example, we employ a transparent conductive film (Cima NanoTech Inc. "SANTE" EMI Shielding Films) having a mesh-like conductor (Fig. 23(a)). Here, tablet devices usually employ capacitive-sensing methods to allow interaction with the touch screen. This means that we may not be able to input data from the touch screen if the shield fully covers the display directly. To mitigate such problems, we introduce a polarization filter of a certain thickness and insert it between the shield material and the touch screen, as shown in Fig. 23(b). Thus, we can reduce the electrical coupling between the shield material and the touch screen and therefore allow input of data to the touch screen. If insufficient reduction is achieved, we change the mesh size of the shield material. Since both films are clear, the countermeasure will work from both electrical and visual viewpoints.

Figure 24 shows the results of reconstructed images at 50 cm away from the tablet with and without the countermeasure. We confirmed that the countermeasure successfully shielded EM radiation from the tablet. Thus, we can prevent EM display stealing by applying an appropriate shield, which greatly attenuates the leakage frequency.

In this section, we examined an electric countermeasure to suppress the EM radiation. It would also be useful to combine it with software-level countermeasures as shown in [3][24].

6. CONCLUDING REMARKS

This paper presented the threat of display stealing through the EM field emitted from tablet PCs. A portable setup with profiling and signal processing techniques enables such EM display stealing in a general and real-time manner. This paper also demonstrated through an experiment that the proposed method could be applied to arbitrary devices of a known model if the model's parameters were profiled in advance. Another experiment showed that the proposed method is available, even at 2 m away from the target PC. The results suggest that quite a lot of tablet PCs can be vulnerable to the attacks in public spaces since the variety of tablet PCs (by usage) is not large. The typical attack scenarios and the possibility for other products were discussed on the basis of the above setup.

This paper also discussed a mechanism of EM emanation from tablet PCs and a countermeasure against the EM display stealing that relies on those emanations. One reason for the information leakage was explained from the EM intensity distribution for a specific leakage frequency. Noise suppression techniques in the EMC field, such as the EM shields in Section 5, were examined for a possible countermeasure against such threats.

All the components in our setup are commercially available, and each profiling/signal processing technique does not include any significant novelty. That's why such EM display stealing can be a practical threat. The threat of EM display stealing from tablet PCs has not been discussed in conventional studies because tablet PCs have weaker EM emissions than conventional PCs do and such weaker EM emissions seems to be reduced to the noise floor quite close to the devices. However, our experimental results clearly identify the security hole of tablet PCs based on such EM emissions.

On the other hand, there are several products naturally resistant to the EM display stealing. Therefore, a future study will be to examine the possibility for and limitation of EM display stealing by a portable setup whose components (e.g., antenna) and pre/post processing techniques are optimized for specific products. In addition, future studies still remains for comprehensive and detailed analysis of information leakage mechanisms for various products with reverse engineering, which would lead to the development of more effective countermeasures.

7. REFERENCES

- [1] NACSIM 5000: Tempest Fundamentals. National Security Agency, Fort George G. Meade, Maryland, February 1982. Partially declassified transcript: <http://cryptome.org/nacsim-5000.htm>
- [2] Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," *Computers & Security*, Vol. 4, pp. 269-286, 1985.
- [3] M.G. Kuhn, Ross J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," *Information Hiding*, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124-142, ISBN 3-540-65386-4.
- [4] M.G. Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays," *Proceedings 2002 IEEE Symposium on Security and Privacy*, Berkeley, California, 12-15 May 2002.
- [5] M.G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays," *4th Workshop on Privacy Enhancing Technologies*, Proceedings, LNCS 3424, pp. 88-105, 2004.
- [6] M.G. Kuhn, "Security Limits for Compromising Emanations," *Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005)*, LNCS 3659, pp. 265-279, 2005.
- [7] M.G. Kuhn, "Compromising emanations of LCD TV sets," *IEEE International Symposium on Electromagnetic Compatibility (EMC 2011)*, pp. 931-936, 2011,
- [8] H. Sekiguchi, and S. Seto, "An evaluation method of the display image reconstructed by electromagnetic emanation," *Proc. of EMC Europe Workshop 2007*, CD-ROM, no. abs-133, 2007.
- [9] H. Sekiguchi, and S. Seto, "Proposal of information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer," *Proceeding of the 2008 IEEE International Instrumentation & Measurement Technology Conference*, Victoria, Canada, May 2008.
- [10] H. Sekiguchi, "Information leakage of input operation on touch screen monitors caused by electromagnetic noise," *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium*, pp.127-131, 2010.
- [11] H. Sekiguchi and S. Seto, "Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment," *Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on*, vol., no., pp.942-945, 2011.
- [12] T. Tosaka, Y. Yamanaka, and K. Fukunaga, "Method for Determining Whether or Not Information Is Contained in Electromagnetic Disturbance Radiated from PC Display," *IEEE Transaction on Electromagnetic Compatibility*, Vol. 53, No. 2, pp. 318-324, 2011.
- [13] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, M. Hattori, "Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer," *Electromagnetic Compatibility, 2006. EMC-Zurich 2006. 17th International Zurich Symposium*, pp.630-633, 2006.
- [14] M. Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless

- Keyboards," Proc. 18th USENIX Security Symposium, 2009, pp.1-18.
- [15] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium, pp.121-126, 25-30 July 2010.
- [16] International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), "K.84: Test methods and guide against information leaks through unintentional electromagnetic emissions," 2011.
- [17] T. Watanabe, K. Franke, H. Sako, "Towards large-scale EM-leakage evaluation by means of automated TOE synchronisation," IEEE International Symposium on Electromagnetic Compatibility (EMC 2011), pp. 937-941, 2011.
- [18] R. O. Duda, and P. E. Hart, "Pattern Classification and Scene Analysis," Wiley, 1973.
- [19] R. O. Duda, and P. E. Hart, "Use of the Hough transformation to detect lines and curves in pictures," Communications of the ACM, vol. 15, no. 1, pp. 11--15, 1972.
- [20] D. M. Hockanson, J. L. Drewniak, T. H. Hubing, T. P. VanDoren, F. Sha, and M. J. Wilhelm, "Investigation of fundamental EMI source mechanisms driving common mode radiation from printed circuit boards with attached cables," IEEE Transactions on Electromagnetic Compatibility, vol. 38, no. 4, pp. 557--576, Nov. 1996.
- [21] T. Watanabe, O. Wada, T. Miyashita, and R. Koga, "Common-mode current generation caused by difference of unbalance of transmission lines on a printed circuit board with narrow ground pattern," Inst. Electron. Inform. Commun. Eng. Trans. Commun., vol. E83-B, no. 3, pp. 593--599, 2000.
- [22] H. W. Shim and T. H. Hubing, "Model for estimating radiated emissions from a printed circuit board with attached cables due to voltage-driven sources," IEEE Transaction on Electromagnetic Compatibility, vol. 47, no. 4, pp. 899--907, Nov. 2005.
- [23] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage and J.-L. Danger, "Analysis of Electromagnetic Information Leakage from Cryptographic Devices with Different Physical Structures," IEEE Trans. on Electromagnetic Compatibility, vol. 55, No. 3, pp. 571-580, June 2013.
- [24] T. Watanabe, H. Nagayoshi, T. Urano, T. Uemura, H. Sako, "Countermeasure for electromagnetic screen image leakage based on color mixing in human brain," 2010 IEEE International Symposium on EMC, pp.138-142, Jul. 2010.