2008 IEEE Symposium on Security and Privacy

Compromising Reflections
– or –
How to Read LCD Monitors Around the Corner

Michael Backes
Saarland University and
Max Planck Institute for Software Systems
Saarbrücken, Germany
backes@cs.uni-sb.de

Markus Dürmuth   Dominique Unruh
Saarland University
Saarbrücken, Germany
{duermuth,unruh}@cs.uni-sb.de

Abstract

We present a novel eavesdropping technique for spying at a distance on data that is displayed on an arbitrary computer screen, including the currently prevalent LCD monitors. Our technique exploits reflections of the screen's optical emanations in various objects that one commonly finds in close proximity to the screen and uses those reflections to recover the original screen content. Such objects include eyeglasses, tea pots, spoons, plastic bottles, and even the eye of the user. We have demonstrated that this attack can be successfully mounted to spy on even small fonts using inexpensive, off-the-shelf equipment (less than 1500 dollars) from a distance of up to 10 meters. Relying on more expensive equipment allowed us to conduct this attack from over 30 meters away, demonstrating that similar attacks are feasible from the other side of the street or from a close-by building. We additionally establish theoretical limitations of the attack; these limitations may help to estimate the risk that this attack can be successfully mounted in a given environment.

1. Introduction

Side-channel attacks are a particularly salient approach for spying on confidential data. As early as in 1985, electrical emanations of CRT screens were successfully exploited to reconstruct the screen's content from a distance [12]. This attack was further refined in diverse variations of different levels of sophistication, e.g., emanations from the cable connecting an LCD screen to the computer were successfully abused to recover the content of the screen [6]. All these attacks are grounded on the idea that an unexpected emanation of the computer itself (or its display) is exploited. These attacks can often be successfully prevented by shielding the hardware to avoid the occurrence of these unexpected emanations, e.g., by using LCD displays instead of CRT screens, by using specially insulated cables, by using soundless keyboards, and so on.

Our work introduces a side-channel that is not an idiosyncrasy of the computer's behavior, but it exploits the visual emanation of the screen itself – and hence its proper functionality – in combination with everyday objects that are located in close proximity to the screen such as tea pots, eyeglasses, plastic bottles, spoons, or the eye of the user. Our approach is predicated on the idea that the image of the screen can be reconstructed from reflections on those objects, see Figure 1. We focus on the (common) setting in which the screen is facing away from the window, see Figure 2, and on curved reflection surfaces, since reflections on these surfaces cover a very large area of the environment; this increases the likelihood that a reflection of the screen's content can be eavesdropped on the object.

We demonstrate in this paper that this idea can be successfully realized in practical scenarios, using inexpensive, off-the-shelf equipment of less than 1500 dollars (a camera and a telescope) from a distance of up to 10 meters for spying on small fonts. Relying on a more expensive telescope allowed us to conduct this attack from over 30 m away. Particularly good results were obtained from reflections in a user's eyeglasses or a tea pot located on the desk next to the screen. Reflections that stem from the eye of the user also provide good results. However, eyes are harder to spy on at a distance because they are fast-moving objects and require high exposure times.

Our experiments indicate that this shortcoming can be remedied by using more expensive equipment that

978-0-7695-3168-7 /08 $25.00 © 2008 IEEE
DOI 10.1109/SP.2008.25

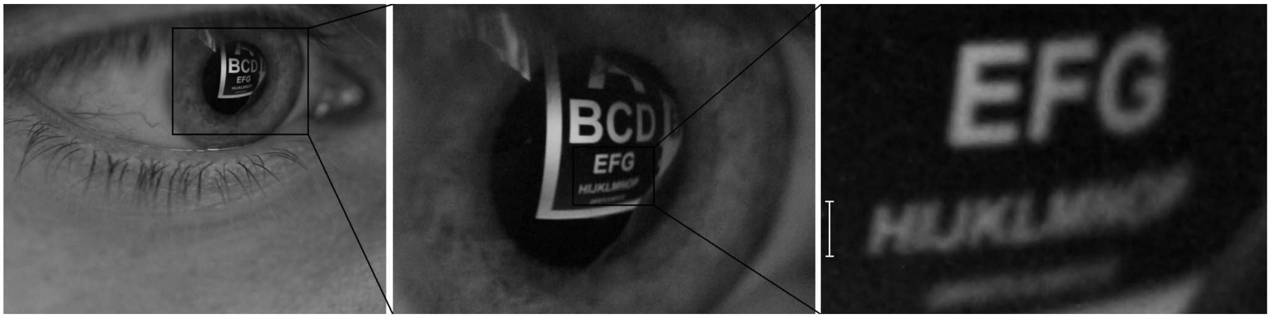

Figure 1. Image taken with a macro lens from short distance; the distance between the eye and the monitor was reduced for demonstration. Readability is essentially limited by the camera resolution.

offers lower exposure times. Unlike the human eye, glasses constitute an ideal target for our attack due to their less extreme curvature. Additionally, we illustrate that reflections of non-emissive objects, e.g., papers that are located on the desk in close proximity to a tea pot, can be exploited to spy on this object; this might allow for spying on confidential documents for which no direct line of sight is given.

We have established lower bounds on the size of the telescope (and consequently the amount of money) needed to carry out this attack in different scenarios. The lower bounds rely on physical characteristics such as diffraction (Rayleigh's Criterion) as well as bounds on the permitted exposure times.

From our experiments, we conclude that the reflections gathered from curved surfaces on close-by objects indeed pose a substantial threat to the confidentiality of data displayed on the screen. Fully invalidating this threat without at the same time hiding the screen from the legitimate user seems difficult, without using curtains on the windows or similar forms of strong optical shielding. Most users, however, will not be aware of this risk and may not be willing to close the curtains on a nice day.

1.1. Related Work

Military organizations have been rumored to deal with compromising emanations since the 1960's; the results of these works, however, are confidential. The first publicly known attack we are aware – published in 1985 [12] – used electromagnetic radiation of CRT monitors. An early discussion of these results can be found in [4].

Various forms of emanations have since been exploited to spy on confidential data. Electromagnetic emanations have turned out to constitute a security threat to computer equipment such as poorly shielded RS-232 serial lines [11], keyboards [1], as well as the digital cable connecting modern LCD monitors [6]. We refer to [7] for a discussion on the security limits for electromagnetic emanation. Acoustic emanations were shown to reveal text typed on ordinary keyboards [2, 13], as well as information about the CPU state and the instructions that are executed [10]. Acoustic emanations from printers were studied in [3].

The work that comes closest to ours is that diffuse reflections of the light emitted by a CRT monitor can be exploited to recover the original monitor image [5]. This approach exploits the point-wise image construction and the time-characteristics of the light-emitting material used in CRT monitor. This technique hence does not apply to monitors that do not construct images in this fashion; in particular, it does not apply to LCD monitors. Information leakage from status LEDs is studied in [8]. Reflections of images from a human eye were already investigated in [9], but without security questions in mind, in particular only for low resolutions, small distances, and without taking diffraction into account.

1.2. Outline

Section 2 reviews the relevant optical parameters and describes their influence on images quality. Section 3 contains our experimental results in various scenarios for the low-cost equipment. Section 4 shows that the approach scales to larger distances by relying on a more expensive telescope. Section 5 establishes theoretical lower bounds on the size of the telescope (and consequently the amount of money) needed to carry out this attack in different scenarios, while Section 6 discusses the feasibility of our attack in realistic scenarios. Section 7 concludes the paper and outlines future work.

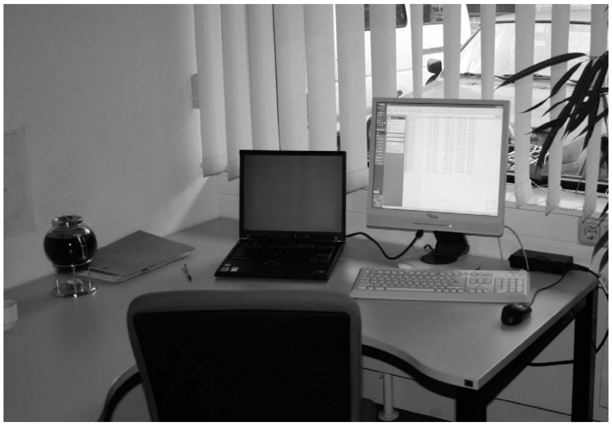

Figure 2. The basic setting: The monitor faces away from the window in an attempt to hide the screen's content.

2. An Optics Primer

We start by reviewing the relevant parameters of the optical system and describe their influence on image quality. This allows us to better understand our experimental results, and it will provide the basis for deriving lower bounds on the resources that are required to mount the attack.

2.1. Size of the Reflected Image

The reflection of an object, in our case a computer display, in a curved mirror creates a virtual image that is located behind the reflecting surface. For a flat mirror this virtual image has the same size and is located behind the mirror at the same distance as the original object. For curved mirrors, however, the situation is more complex. In this section, we calculate the size and the location of the virtual image.

The overall situation is depicted in Figure 3. It is common to approximate a spherical mirror as a lens of focal length $f_0 = \frac{r}{2}$, provided that the width of the mirror is small compared to its radius. The location b_0 of the virtual image (the distance between the virtual image and the reflecting surface), given the location a_0 of the object, is given by the *thin lens equation* as

$$b_0 = \frac{1}{\frac{2}{r} - \frac{1}{a_0}}.$$

The size u_0 of the virtual image is given by $u_0 = \frac{b_0 x}{a_0}$. Finally, we have to consider that the image appears smaller if seen from an angle γ; the *apparent size* u_1 is $u_1 = u_0 \cdot \cos(\gamma)$.

Let the distance from the monitor to the observer be d, and let n be the desired resolution; the desired resolution could be the actual monitor resolution, but it could also can be lower, depending on the scenario. In the following we will mainly use the full resolution, but we will later discuss how these results scale with a lower resolution. The optical resolution α (in radians) required to capture the full resolution is given by $\alpha = \arctan \frac{u_1}{nd} \approx \frac{u_1}{nd}$, where the approximation holds as $u_1 \ll d$ and $\tan \alpha \approx \alpha$ for $\alpha \approx 0$. In particular, α is linear in the inverse of the distance d.

2.2. Diffraction Bounds

Diffraction is a physical phenomenon that diffuses light, or any other electromagnetic wave, whenever it passes some aperture. It is best known for very small apertures, where it is visible to the human eye. In the case of high magnifications, however, even a large aperture like the one of a telescope produces noticeable diffraction; in fact, the diffraction constitutes one of the limiting parameters in the use of modern telescopes.

The influence of diffraction on the maximum resolution of a telescope is given by *Rayleigh's Criterion.* Let two point sources P_1, P_2 be given such that the angle between these two sources (as seen by the observer) is α (in radians). Let D be the diameter of the objective lens of the telescope and λ the wavelength of the light. Then Rayleigh's Criterion states that the two points P_1, P_2 can be distinguished if and only if $\alpha \geq \frac{1.22\lambda}{D}$. In some of our experiments we were close to the theoretical bound given by Rayleigh's Criterion. Combining the bounds from this section and from the previous one, we obtain bounds on the maximum resolution for a given distance and telescope aperture.

2.3. Exposure Time

Another important factor in our experiments turned out to be the necessary exposure time. Since the exposure time depends on many practical factors in the setup (quality of the lenses, brightness of the screen, color of the reflecting object, sensitivity of the film/chip in the camera, etc.) it does not seem possible to give reasonable theoretical bounds on the exposure time. It is known, however, that the exposure time is inversely proportional to the intensity of the light per square angle reaching the camera. Thus if all other values are fixed, the necessary exposure time is proportional to the square of the magnification and inversely proportional to the square of the aperture diameter. (The distance does not directly influence the exposure time, but a larger distance will usually be compensated by

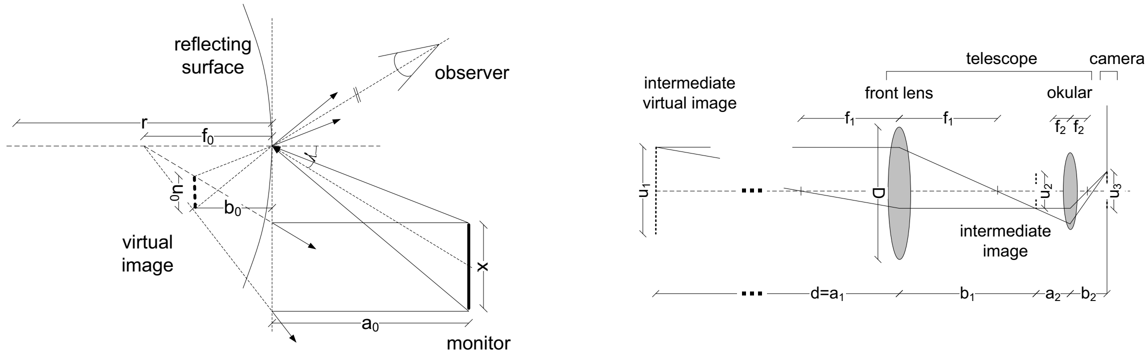

Figure 3. Size and location of the reflected image. The curvature of the sphere in the left part of the figure is exaggerated for illustration.

a larger magnification, hence indirectly influences the exposure time.) Given experimental values for a given setup, this allows us to at least estimate the necessary exposure time for settings that vary only in these parameters, e.g., when deciding which telescope size is necessary for a given setup. Furthermore, by comparing our equipment with other available equipment, we at least obtain an estimate when the attacker does not use specifically manufactured (and possibly very expensive) equipment.

In theory, there is no upper bound on the exposure time. However, changing monitor images, moving objects, and air turbulences caused by heating or air conditioning can blur the image. Exposure times of several seconds are possible; we have taken most pictures with exposure times of two seconds. For moving mirrors, in particular for the human eye, much shorter exposure times are required, as the rapid movement of the eye substantially blurs images even after a 0.1 seconds.

3. Experimental Results for Low-cost Equipment

We now present experimental results using low-cost equipment that illustrate the feasibility of the attack. The experiments show that many objects that may be found at a usual workplace can be exploited to retrieve information on a computer's display by an outsider.

In the following, we consider the test image depicted in Figure 4 shown on the 15" LCD screen of a ThinkPad T43. We then placed a reflecting object on the table close to the LCD screen (except for the cases where we investigated the reflections in the eye of the user) and photographed the reflection of the screen in the object from various distances through a telescope.

We used the following camera and two telescopes for our tests:

- An SLR digital camera Canon EOS 400D with a resolution of 10.1 mega-pixels and a sensor size of $22.2mm \times 14.8mm$; it costs approx. 550 Euros (800 dollars).

  Some pictures were taken using a Sigma macro lens with focal length $f = 50mm$ and an approximate aperture of $D = 18mm$ ($F = 2.8$). Using this lens with a smaller sensor yields a slightly cropped image, comparable to images taken with an $80mm$ lens.

- A refractor telescope: a Skywatcher ED 80 PRO with focal length $f = 600mm$ and an aperture of $D = 80mm$. This telescope has very good imaging qualities, but a quite small aperture. Its price is approximately 380 Euros (550 dollars).

- A Newtonian reflector telescope: a Skywatcher Dobson 200 with focal length $f = 1000mm$ and an aperture of $D = 200mm$. Its simple design has impacts on image quality, mostly on color fidelity and distortion, which both are of only minor importance for our task. Its larger diameter, however, allows for a higher resolution according to Rayleigh's Criterion and for shorter exposure times. It costs approx. 300 Euros (435 dollars). Unless explicitly stated otherwise, the experiments described below were conducted using this telescope.

Both telescopes were used with the Canon EOS 400D, directly mounted on the telescope with a projection camera adapter using a $25mm$ eye piece and extension tubes to allow for the short object distances. The camera was triggered by remote control and configured to

Figure 4. The test image used in most of our experiments. Font sizes are 300pt, 150pt, 72pt, 36pt, and 18pt.

wait between moving its mirror and taking the actual photo (mirror lockup) to reduce the effect of vibrations.

We have investigated the following reflecting objects: Various tea pots, human eyes, eyeglasses, drinking glasses, bottles, and spoons. In the following we describe the results obtained with these objects.

3.1. Reflections in Tea Pots

We obtained very good reflections in various tea pots. We frequently used the tea pot shown in Figure 5, which is the tea pot that one of the authors uses daily. Figure 6 shows two additional tea pots that we investigated.

The reflections shown in Figure 5 and Figure 6 as well as in most of the following figures were taken indoors. At the time of most of the experiments, the outdoor and indoor temperatures differed by approximately 20 degrees Celsius and poorly insulated windows caused heavy air turbulence. In combination with the quite long exposure time of one second, this caused blurred images, so we photographed the reflections indoors. Our experiments on a warmer day indicate that this does not constitute a serious problem, as it does not occur when temperatures outside are warmer, when better insulated glass is used, or when sensors of higher sensitivity are used, which leads to shorter exposure times. Alternatively, one can resort to a technique used in astronomical photography, where air turbulences cause blurred images: Many images are taken with very short exposure times; Each of these images is heavily underexposed, but subject to very little blur. Then approx. 10% of the best images are added to obtain a single, bright and unblurred image.

Figure 7 shows the reflection of a Word document with a font size of 12pt, from a distance of 5 meters.

3.2. Reflections in Human Eyes

Another reflecting object that is prevalent in all offices is the human eye. In fact, the reflecting properties of the cornea, the foremost part of the human eye, are excellent, as it is designed not to distort the light beams passing it (this can be seen in Figure 1). On the downside, the radius of the cornea is very small, and the reflection is quite dark, requiring long exposure times.

The rapid movement of the eye causes the images taken with our equipment to be rather blurred when taken from a distance, see Figure 8. For photographing reflections in the eye a high magnification is used. Since the eye itself does not reflect much light, the exposure time constitutes the limiting factor in these experiments.

Figure 9 shows the reflections from a short distance, taken with a macro lens, where the eye is at a normal distance from the monitor. The readability of the text is essentially limited by the resolution of the captured image. (The bar in the rightmost picture has a height of 18 pixels, consequently the line below was recorded with a resolution of 9 pixels. Although this does not (yet) constitute a practical attack, it serves as a strong indication that the reflections are of high quality, and that they could be captured using more expensive equipment.

3.3. Reflections in Eyeglasses

Eyeglasses are another prevalent reflecting object. In fact, glasses substantially facilitate the attack, as they typically have surfaces with a large radius. It turned out that even anti-reflecting coatings do not disturb the attack. The pictures in Figures 10 were taken while the glasses were worn by their respective owner. Both glasses had an anti-reflecting coating.

3.4. Reflections in Other Objects

Surprisingly many objects yield suitable reflections. The following three examples were captured from a distance of 5 meters. The reflections in an empty wine glass are shown in Figure 11. The double reflections are caused by the two faces of one side of the glass. As the radii of both surfaces are essentially equal, both reflections can be seen sharply. The other side of the glass cannot be seen. A glass full of wine would offer even better reflections, because of the darker background. An ordinary plastic bottle produces reasonable reflections as well, see Figure 12. Depending on the exact position and the exact shape of the bottle, the image can be distorted; in some cases even the last line is

Figure 5. Reflections in a tea pot, taken from a distance of 10m. The 18pt font is readable from the reflection.

Figure 6. Reflections in two other tea pots, taken from a distance of 5m. The 18pt font is readable from the reflection in the left picture, and almost readable in the right picture.

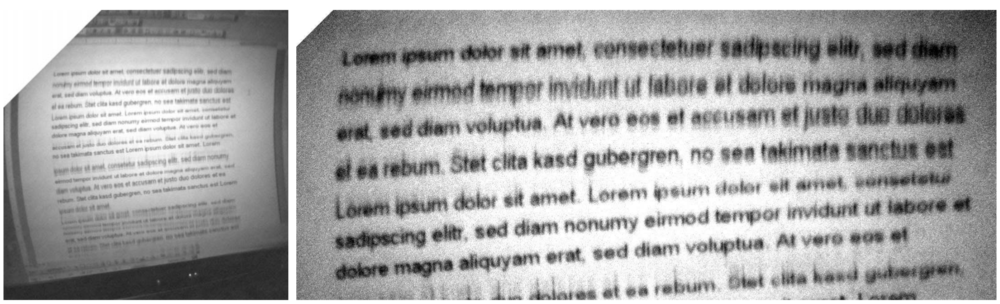

Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.

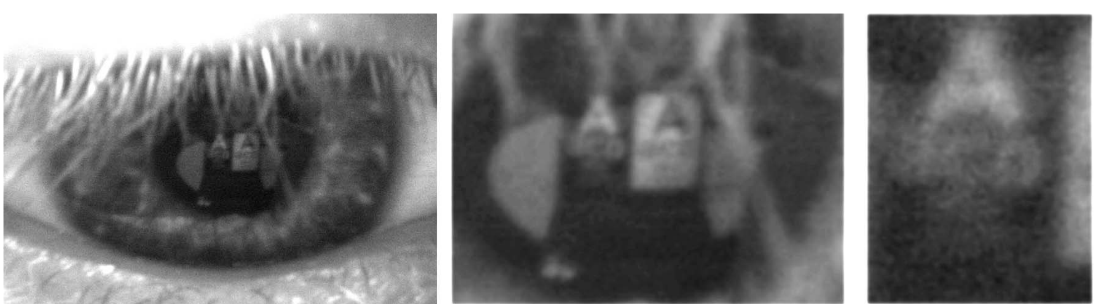

Figure 8. Image taken with the refractor telescope from a distance of 3.5m, produced with an exposure time of one second.

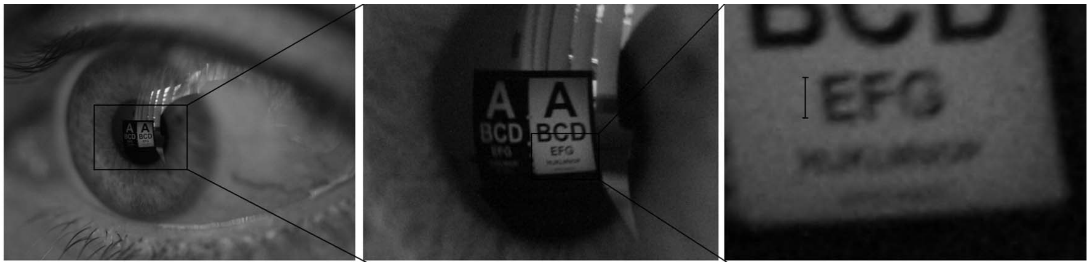

Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.

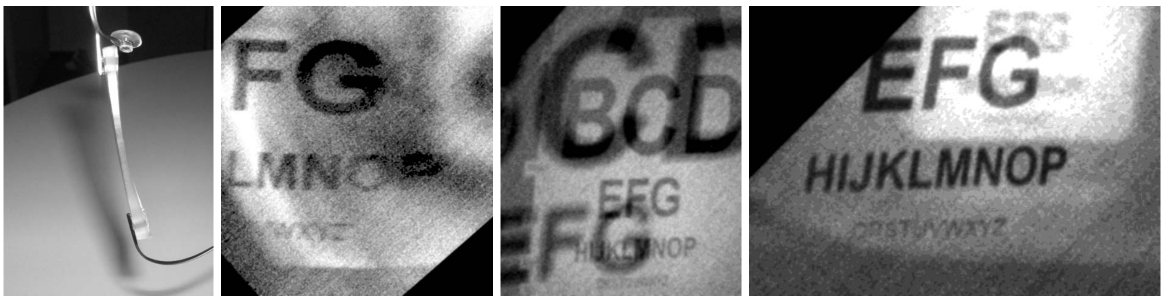

Figure 10. Reflections in two different pairs of glasses, taken from a distance of 5m. Both the inner side and the outer side of glasses produce reflections. The 18pt font is readable from the reflection.

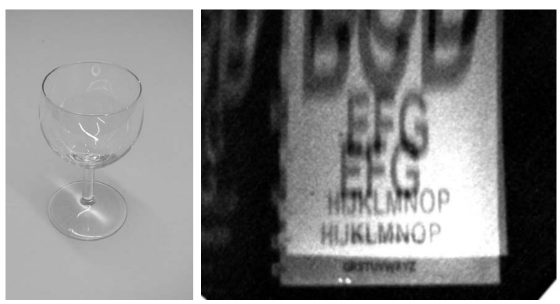

Figure 11. Reflections in an empty wine glass, taken from a distance of 5m. Reflections occur on both sides of the glass. The 18pt font is readable from the reflection.

Figure 12. Reflections in a 0.5l plastic Coca-Cola bottle, taken from a distance of 5m. Because of the irregular surface, only parts of the text are readable.

readable. Even a spoon has clear reflections, both on its inner and outer side, see Figure 13.

3.5. Printouts Reflecting in a Tea Pot

Although a tea pot theoretically can reflect all the objects in a room, and our work shows that it reflects the monitor quite well, the monitor is a bright target compared with paperwork lying on the desk. Figure 14 shows that the tea pot also reflects paperwork and could be used to cover cases where the attacker does not have a direct view on the paper. In Figure 14, the paper was placed next to the tea pot and the work space was lit by an ordinary desk lamp. In this case, the paper and the reflecting object (tea pot) were very close and the image quality is excellent. One can easily read the reflection of the 10pt font paper.

3.6. Large Distances

For distances beyond approx. 10 meters between reflector and camera, diffraction substantially limits the resolution we can obtain with our low-cost telescope (cf. Section 5 and Table 1). Of course one could simply use a larger telescope, but even the substantially lower resolution can impose a substantial threat. Figure 15 shows two images captured over a distance of 40 meters in which graphical information is clearly readable, e.g., business charts. At the authors' campus, this is the distance between two computer science buildings, which means that this quality is realistic when spying from one building to the other.

4. Experimental Results for More Expensive Equipment

We now present experimental results using more expensive equipment: a Dobson telescope of excellent quality with mirror diameter $D = 60cm$ and focal length $f = 2.6m$. A used telescope sells for about 19'000 Euros (approx. 27'500 dollars). The telescope is shown in Figure 16, along with an image of the reflections in a tea pot from a distance of 30 meters. The quality of the captured image is compliant with the following theoretical observations. The Rayleigh Criterion gives a linear correlation between the telescope diameter and the distance where images of a constant quality can be taken. Furthermore, the brightness of the image decreases quadratically when the distance increases, and the area of the mirror, i.e., its capability to gather light, increases quadratically with increasing mirror diameter. Thus overall, the relation between distance and mirror diameter is also linear.

Reflecting objects (radius r)	Distance d to the camera	Minimal aperture D
Tea pot ($70mm$)	5m	16.6cm
Tea pot ($70mm$)	10m	33.2cm
Human eye ($8mm$)	2m	62cm
Human eye ($8mm$)	5m	155cm
Human eye ($8mm$)	10m	310cm

Table 1. Some concrete values for the minimal aperture D needed to capture the full resolution of 1024 pixels.

5. Practical Limits of this Approach

To better understand the implications of this attack and for providing concerned people with suitable defense mechanisms it is important to study the principal limitations of our approach. Our bounds are not absolute, but they depend on the size of the telescope. However, since the price tag of the telescope is directly related to its size, one can at least estimate a lower bound for the costs of an attack in a given setting. Furthermore, in many settings there might be an upper bound on the size of the telescope because the telescope needs to be hidden somewhere.

5.1. Based on the Rayleigh Criterion

The first lower-bound can be derived from the Rayleigh Criterion, cf. Section 2.2. We have

$$D \geq \frac{1.22\lambda}{\frac{u_1}{nd}} = \frac{1.22\lambda nd}{u_1} \qquad \text{for} \quad u_1 = \cos(\gamma) \cdot \frac{\frac{1}{\frac{2}{r} - \frac{1}{a_0}} x}{a_0}.$$

For illustration we give some concrete values in Table 1. These values are for the full resolution $n = 1024$ pixels; the monitor width $x = 30cm$, the monitor distance (from the eye) $a_0 = 50cm$, the wavelength $\lambda = 600nm$, and the angle $\gamma = 0$ are kept constant. In most cases a fraction of the full resolution is sufficient to achieve good results, in this case the distance *or* the diameter can be multiplied/divided by a corresponding factor.

An increasing diameter has two negative effects for the attacker: First, the telescope gets increasingly large. Typically the focal length of telescopes increases linearly with the diameter, making it difficult to hide the telescope. Second, the prices of these telescopes increase rapidly with increasing diameter. For astronomical telescopes, the most expensive part is the mirror (lenses are even more expensive and hardly ever used in large astronomical telescopes). Thus we consider

Figure 13. Reflections at the inner side and at the outer side of a spoon, taken from a distance of 5m. The 18pt font is readable from the reflection in the right figure, and almost readable in the left figure.

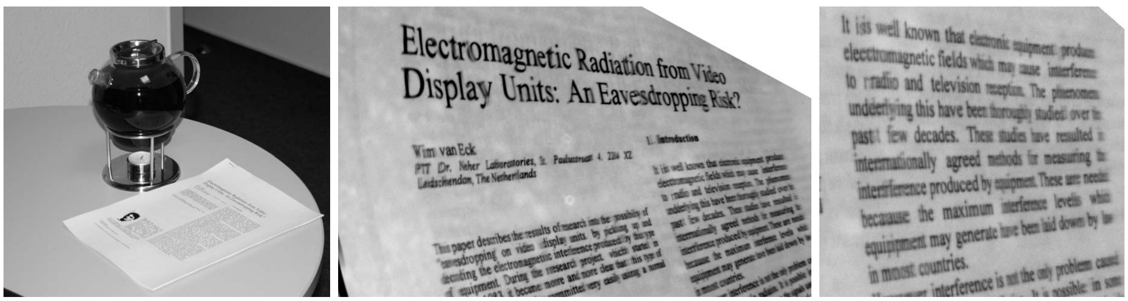

Figure 14. Reflections of a printed paper in a tea pot, taken from a distance of 5m. The paper was located close to the tea pot, yielding excellent reflections.

Figure 15. Reflections of the monitor in a tea pot, taken from a distance of 40 meters. Readability is good enough to identify relevant information from, say, business charts.

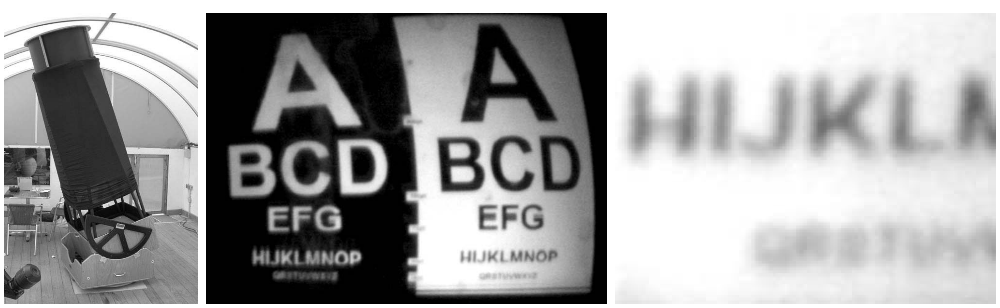

Figure 16. Reflections in a tea pot, taken from a large distance of 30 meters using a larger telescope. The 18pt font is readable from the reflections.

the price of the mirror only; prices of three randomly selected manufacturers are shown in Figure 17. (Note that prices for mirrors of the same size can vary depending on the manufacturer, the quality, and finishing.)

The Rayleigh Criterion was specifically stated for the human eye. The imaging quality of typical telescopes is lower than the Rayleigh Bound, due to inaccuracies of lenses and mirrors. With the assistance of cameras and post-processing one could perhaps improve on the resolution. However, even with expensive equipment, we expect the Rayleigh Bound to be correct up to a small constant factor.

Another possible attack scenario would be to use techniques from astronomy to increase imaging quality, in particular an array of telescopes or mirrors as in the Very Large Telescope Project. This technically challenging undertaking is typically only used for telescopes with a diameter greater than 5 meters. An array of 5 meter telescopes is unrealistic in our attack scenario, and the technical challenges of a portable telescope array are unlikely to be resolved at a reasonable price.

5.2. Based on the Exposure Time

In our experiments, the exposure time was the limiting factor in photographing reflections in the human eye. The reflection in the eye is very small, thus large magnification is needed. As discussed in Section 2.3, the exposure time grows quadratically with the magnification.

Deriving bounds based on the exposure time, similarly to what we did in the previous section for the diameter, depends on the quality of the photographic film/chip an other factors that are hard to measure. The exposure time seems to be the actual limiting factor in some of our experiments, and we know that exposure time is proportional to the square of the magnification and inversely proportional to the square of the aperture diameter. We can thus extrapolate values of the exposure time to get an impression about the limits incurred by the necessary aperture time. One should keep in mind that bounds obtained in this fashion are correct only assuming a camera of the same quality as our and assuming that no special algorithmic techniques are used to reconstruct the screen from sequences of underexposed pictures.

6. Threat Analysis

6.1. Possibility of Improvement

The experimental results presented in this paper are only a first case study. The most obvious improvement is to use more expensive hardware: a larger telescope with larger diameter and a more sensitive camera to improve the exposure time. Also methodical and algorithmic improvements are possible. So far, we have photographed the pictures and applied simple standard algorithms to improve readability. However, advanced deconvolution algorithms or the analysis of whole sequences of pictures might lead to much better picture quality. For instance, in astronomy there is a technique called "lucky imaging" where several underexposed pictures are algorithmically combined to yield a picture of higher quality, see Section 3.1.

A single picture of the whole screen is also not necessary; one could shoot a series of photos and combine them in a jigsaw puzzle fashion. We conjecture that the attack can be improved by at least one order of magnitude in both resolution and distance by applying a combination of such techniques.

6.2. Low Resolution

Even if improvements on our technique are not sufficient to increase the resolution such that small fonts on a screen are readable, there are still threats beside the possibility to read mere text. For example, even with a very unclear picture of the screen it might be possible to guess which program a user is currently using, or even to recognize web pages the user is currently browsing. The latter in particular works if there is a limited set of possible candidates with which to compare the layout on the screen. As soon as such a web page is found, one can follow the browsing user by only clicking on links, since the set of links on a given page typically yields a small list of candidates.

Furthermore, presentations generally use very large fonts and could easily be read from a distance, compromising sensitive business information. If the attacker has good contextual knowledge, even blurred diagrams and graphs can reveal damaging information, e.g. a bar chart showing confidential sales figures. In these cases, even the low resolution we achieved when photographing the human eye might already pose some threat.

6.3. Disguise

Standing with a large telescope directly in front of the user and observing him obviously causes suspicion. It is essential for the attacker to be unnoticed. Assuming a distance of 10 meters or more, the telescope could be mounted inside a small van parked near the window of the user (assuming a ground floor office). Opacifying the windows of the van except for one window and switching off lights inside, the telescope should not be

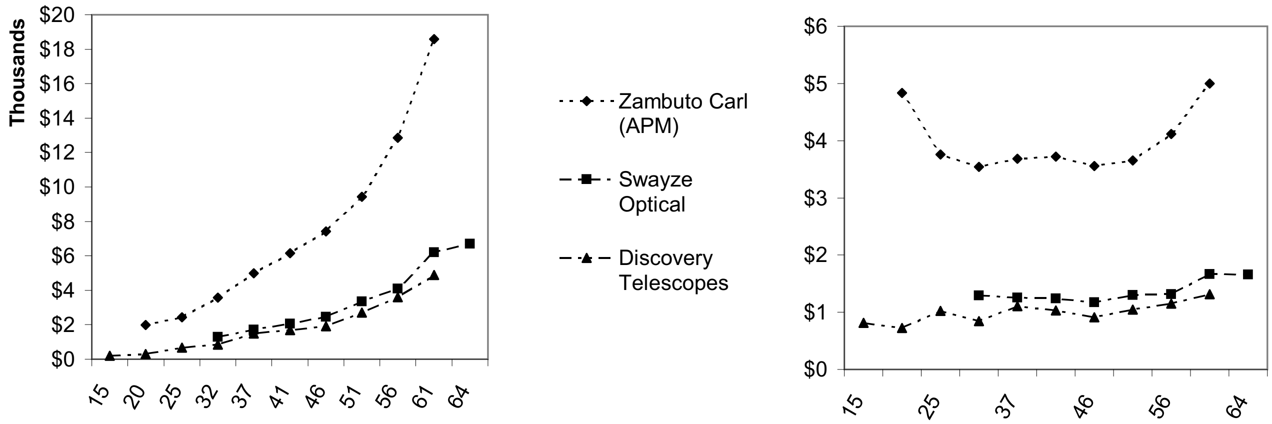

Figure 17. Prices of Newtonian mirrors of various manufacturers for increasing diameter (left side), and per square-cm (right side).

visible. A larger distance of 20-30 meters might even allow to observe the user from an apartment on the other side of the road.

6.4. Availability of reflecting surfaces

Although our experiments were performed under lab conditions, it is realistic that there will be several reflecting surfaces near any given computer. The office of one of the authors had five curved reflecting surfaces: a glass, a bottle, a muesli container, a spoon, and the front glass of a wall clock. More tidy offices might be less threatened but the eye of the user (or even his glasses) will be present.

7. Conclusion and Future Work

We have presented a novel eavesdropping technique for spying at a distance on data that is displayed on an arbitrary monitor, including the currently prevalent LCD monitors. Our technique exploits reflections of the screen's optical emanations in objects that one commonly finds in close proximity to the monitor. This includes glasses, tea pots, spoons, plastic bottles, and even the eye of the user. We have demonstrated that this attack can be successfully mounted using inexpensive, off-the-shelf equipment. Relying on more expensive equipment allowed us to conduct this attack from larger distances; in particular spying from a close-by building clearly becomes feasible.

Particularly good results were obtained from reflections in a user's eyeglasses or a tea pot located on the desk next to the screen. Reflections that stem from the eye of the user also provide good results. However, eyes are harder to spy on at a distance because they are fast-moving objects and require high exposure times. Using more expensive equipment with lower exposure times helps to remedy this problem. We have furthermore established lower bounds on the size of the telescope (and consequently the amount of money) needed to carry out this attack in different scenarios, based on physical characteristics such as diffraction as well as bounds on the permitted exposure times. Fully invalidating the attack seems difficult, except for using curtains on the windows or similar forms of optical shielding.

We are currently conducting experiments on a related attack that is not based on reflecting objects, but rather exploits diffuse reflections on the user's clothes or on a nearby wall. The approach is grounded on the following idea: A single monitor pixel (in particular for LCD displays) produces a slightly directed beam; hence a narrow area of the wall is lightened, which is called the *Point spread function* (PSF). Measuring this function and applying modern deconvolution algorithms both to this function and the image of the light distribution on the wall allow for partial re-computation of the monitor image. Algorithms already exist that behave well if the original image has high contrasts, e.g., text documents on a monitor. While diffuse reflections naturally complicate the situation, first examples indicate that this approach is feasible at least under idealized conditions: A diffusely reflected image of the letter C and the corresponding reconstruction is shown in Figure 18.

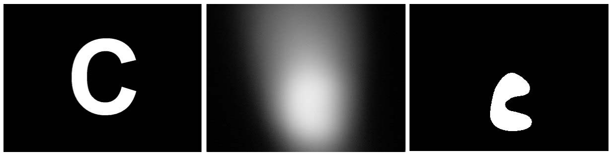

Figure 18. Diffuse reflections of a monitor display from a wall, recovered using deconvolution algorithms: The monitor image (left), the reflection from the wall (middle), and the result from deconvolution, gamma correction, and edge detection (right).

Acknowledgments

We would like to thank Hendrik Lensch and Andrei Linţu for helpful discussions and for giving us access to parts of their telescope equipment, to Markus Ludes from APM Telescopes for giving us access to the 60cm Dobson telescope, and to Markus Kuhn and Jean-Jacques Quisquater for general comments.

References

[1] R. J. Anderson and M. G. Kuhn. Soft tempest – an opportunity for NATO. In *Information Systems Technology (IST) Symposium "Protecting NATO Information Systems in the 21st Century"*, 1999.

[2] D. Asonov and R. Agrawal. Keyboard acoustic emanations. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, 2004.

[3] R. Briol. Emanation: How to keep your data confidential. In *Symposium on Electromagnetic Security for Information Protection*, 1991.

[4] H. J. Highland. Electromagnetic radiation revisited. *Comput. Secur.*, 5(2):85–93, 1986.

[5] M. G. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *Proc. of the 2002 IEEE Symposium on Security and Privacy*, 2002.

[6] M. G. Kuhn. Electromagnetic eavesdropping risks of flat-panel displays. In *Proc. 4th Workshop on Privacy Enhancing Technologies*, pages 88–107, 2005.

[7] M. G. Kuhn. Security limits for compromising emanations. In *Proc. of CHES 2005*, volume 3659 of *LNCS*. Springer, 2005.

[8] J. Loughry and D. A. Umphress. Information leakage from optical emanation. *ACM Transactions on Information and Systems Security*, 5(3):262–289, 2002.

[9] K. Nishino and S. K. Nayar. Corneal imaging system: Environment from eyes. *International Journal on Computer Vision*, 2006.

[10] A. Shamir and E. Tromer. Acoustic cryptanalysis – on nosy people and noisy machines. Online at http://people.csail.mit.edu/tromer/acoustic/.

[11] P. Smulders. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers & Security*, 9:53–58, 1990.

[12] W. van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4:269–286, 1985.

[13] L. Zhuang, F. Zhou, and J.D.Tygar. Keyboard acoustic emanations revisited. In *Proceedings of the 12th ACM Conference on Computer and Communications Security*, 2005.