CS 454 Signature Project, Spring 2024
Report on the News Story, "Tablet's Light Sensor Can Spy on Users"
Sample Assignment Response by Henry M. Walker

In recent years, many news stories have described how a computer's camera, keyboard, and/or microphone might be used by hackers to gain information about a user. This story describes a different threat: Many computers, such as mobile devices and computers, contain ambient light sensors to adjust a monitor's brightness and other qualities. Using this technology, M.I.T. graduate student, Yang Liu, and his colleagues "developed an inversion algorithm to transform readings from such a sensor into a 32x32-pixel image of the region above the display" [1] Even though current images have low resolution and take moderate processing time, analysis of multiple frames can identify basic hand movements, which in turn allow inferences of how a user may be using the device. Altogether, this news story discusses several important themes for consideration, including the underlying purpose of the research, current state of the work, the impact of this technology on users, current policies and practices related to this technology, and ways this technology might evolve in the future.

As an article in IEEE Spectrum discusses, cameras, microphones, and other components of computing-related device might allow applications to learn about users' interests and, in some cases, their private data. In response, users may cover cameras, turn off microphones, or otherwise disable sensors to minimize risks. However, most devices also contain ambient light sensors that measure the amount of background light within an environment. Such sensors are always active, so that a device can adjust the brightness of a screen to match its surroundings. [3] Apparently the underlying research question for Yang Liu and his colleagues was how much information might be inferred by successive readings from this single sensor.

Overall, if specially-created videos are played on a device's screen, light will reflect from a user's hand to the user's head and back to the ambient sensor. Since the video source is known, an algorithm can infer movements of the hands as they work with the tablet. Currently, even though the sensor only identifies a single measurement of light intensity, a sequence of readings can be used to create a low-resolution image of the area above the sensor. This can give a rough image of the hand and also determine common hand gestures when using the device. At present, however, this type of application is quite limited, due to the time required for the required processing.

Overall, the IEEE Spectrum story outlines how, in some circumstances, successive readings can turn the single sensor into a type of low-resolution camera, which might allow discovery of user practices or preferences. For example, this technology "can be used to infer what kind of TV programs someone is watching, what websites they are browsing, or even keypad entries on a touchscreen." [2] Further, since ambient light sensors cannot be turned off, this approach seems to have potential to undermine personal privacy.

Interestingly, the IEEE Spectrum story mentions that past research by security researcher, Lukasz Olejnik, has led the World Wide Web Consortium to recommend limiting access to ambient light sensors. Apparently modern browsers now follow this recommendation. However, Android computers do not have general limitations on such access. Further, "some devices directly log data from the light sensor in a system file that is easily accessible, bypassing the need to go through an API." [2] In short, some computing systems currently seem to be limiting access to the ambient light sensors—likely blocking use of the algorithm(s) described here, but other systems may be quite open to this type of attack.

Looking ahead, one can envision at least two contrasting paths in which the technology described here might evolve.

- Processing time currently is identified as a significant constraint for this use of the ambient light sensor. The article itself notes that this time might be reduced by moving toward lower-resolution images of the hand. Further, improvements in technology might allow processing to proceed more quickly, perhaps with improved algorithms or with multiple processors, .
- Hardware and/or software standards might significantly reduce access to the ambient light sensor, largely blocking the widespread use of the type of application described in the IEEE Spectrum article.

In summary, research by Yang Liu and his colleagues at M.I.T. demonstrates how an ambient light sensor has the potential to be used as a type of camera, allowing the tracking of hand movements and perhaps inferring a user's preferences in working with a device. Altogether, this type of application may have potential as a new risk to personal privacy On the other hand, at present, processing times are relatively long, images have low resolution, and applications are limited. Looking head, advances in technology may address the current limitations. However, policies and practices could be instituted and expanded to block abuses. Either way, this may be an interesting and worthwhile application to follow in the coming years.

References

1. Association for Computing Machinery (ACM), "Tablet's Light Sensor Can Spy on Users", ACM Tech News, URL: https://technews.acm.org/archives.cfm?fo=2024-01-jan/jan-19-2024.html (accessed January 20, 2024).
2. Gent, Edd, "**Your Tablet's Light Sensor Can Spy On You >** A tricky hack demonstrates that even seemingly innocuous components can pose risks", IEEE Spectrum, January 2024, URL: https://spectrum.ieee.org/ambient-light-sensor-cybersecurity-risk (accessed January 20, 2024).
3. Wikipedia, "Ambient Light Sensor", Wikipedia, the Free Encyclopedia, URL: https://en.wikipedia.org/wiki/Ambient_light_sensor" (accessed January 20, 2024). https://en.wikipedia.org/wiki/Ambient_light_sensor#References