Daniel Bachfeld

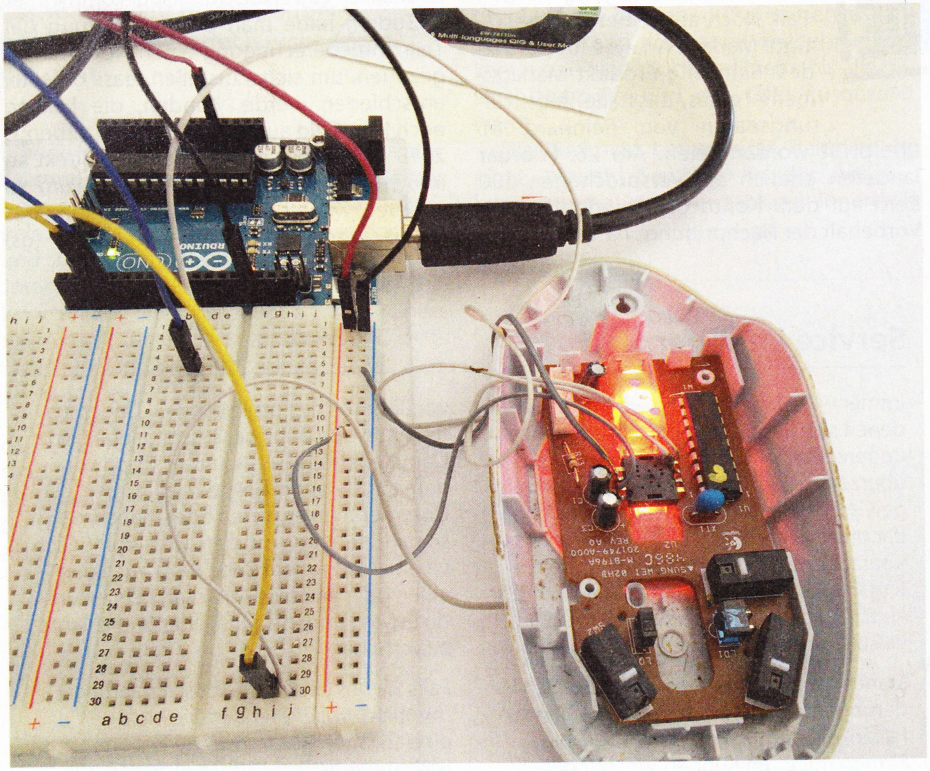
Im Auge der Maus

Computermäuse laden Schädlinge aus dem Netz nach

Kaum sichtbare Mini-Codes auf präparierten Mauspads aktivieren in scheinbar harmlosen optischen Computermäusen eine Spionagefunktion. Ein c't-Test deckt auf, ob die eigene Maus betroffen ist.

Über erste Angriffe auf PCs mit einer trojanischen Maus berichtete c't bereits vor knapp drei Jahren [1]. Eine herkömmliche Maus wurde im Inneren mit zusätzlicher Elektronik ausgestattet. Sobald sie an einen PC gesteckt wurde, fungierte sie zusätzlich als Tastatur-Controller und „tippte" heimlich Befehle ein, um Exploits zu installieren. Mit derart präparierten Mäusen versuchten verschiedene Geheimdienste beispielsweise Hersteller militärischer Produkte auszuspähen. Durch diese Angriffe aufgeschreckt, gingen Sicherheitsverantwortliche in Unternehmen dazu über, nicht nur USB-Sticks genauer unter die Lupe zu nehmen, sondern auch Computer-Mäuse. Wie üblich hat dabei nun ein Katz-und-Maus-Spiel begonnen, in dessen Folge sich die Spione immer neue Tricks ausdenken. Auf einen davon stießen die Kollegen von c't Hacks beim Basteln.

Derart manipulierte Mäuse mit zusätzlicher Elektronik bestehen keinen Test beim Sicherheitsbeauftragten.



Wenn man den Sensor unter Umgehung des USB-Controllers anschließt, kann ein Arduino die Pixeldaten der Kamera einzeln auslesen.

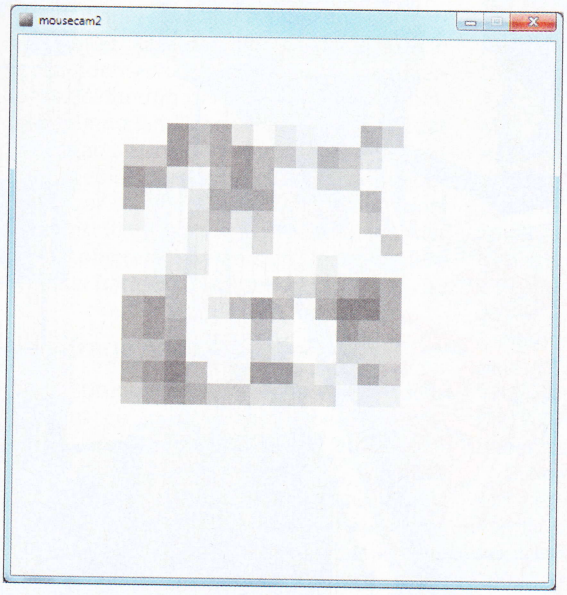
Eigentlich wollten die Kollegen nur eruieren, ob sich für ausgediente optische Mäuse noch eine neue Verwendung finden ließe. Klemmt man beispielsweise einen Arduino unter Umgehung der USB-Schnittstelle direkt an den Maussensor, so lassen sich die Bewegungsdaten für die X- und Y-Richtung auslesen. Der Roboter des c't-Bot-Projekts nutzt diese Methode zur Verbesserung seiner Odometriedaten. Der vielfach in Logitech-Mäusen verbaute Foto-Sensor ADNS-2610 des Herstellers Avago hat 18 × 18 Pixel, ist also eine kleine Kamera, die mehr als 1000-mal pro Sekunde die Oberfläche eines Mauspads oder der Tischplatte fotografiert. Durch Vergleich der Bilder und spezielle Algorithmen (optischer Fluss) ermittelt der Sensor die Bewegungsrichtung und Geschwindigkeit. Praktischerweise kann man die einzelnen Pixeldaten byteweise als sechsbittige Grauwerte aus dem Sensor auslesen, wenn man an USB vorbei direkt mit dem Sensor spricht.

Geisterhand

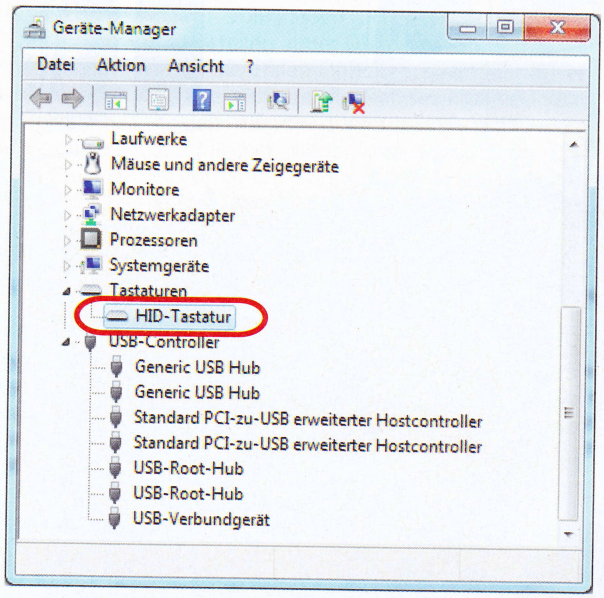
Bei unseren Versuchen, den Sensor als Miniaturkamera für den Arduino zu benutzen, während die Maus selbst noch per USB angeschlossen war, stießen wir jedoch auf ein merkwürdiges Verhalten. Immer wenn der Sensor über bestimmten Stellen auf einem Mauspad schwebte, benahm sich der benutzte Ubuntu-Testrechner seltsam: Das Dashboard öffnete sich und wie von Geisterhand eingetippt erschien eine Folge von Befehlen: `cmd` sowie ein ftp-Befehl nebst einer IP-Adresse und dem Befehl zum Download (`get`) und Start einer Datei. Das Linux konnte damit nichts anfangen, unter Windows hätte jedoch die gesendete Tastenfolge das Startmenü geöffnet, die Eingabeaufforderung gestartet und darin die Datei nachgeladen und ausgeführt.

„Nachtigall, ick hör dir trapsen" – die zu Hilfe gerufenen Kollegen von heise Security luden die Datei manuell herunter und nahmen sie genauer in Augenschein. Bei einer statischen Analyse der Datei auf dem Antivirenportal Virustotal schlug zwar keiner der Scanner Alarm, eine dynamische Laufzeitanalyse offenbarte jedoch, dass es sich um einen ziemlich ausgebufften Windows-Schädling mit Tarnkappenfunktionen handelt. Einmal auf ein System losgelassen, erlaubt er seinen entfernten Schöpfern, die vollständige Kontrolle über Betriebssystem und Peripherie zu übernehmen – nebst Videoüberwachung bei angeschlossener Webcam.

Offenbar handelt es sich bei der von uns gefundenen Maus um eine Schläfermaus, die so lange als normales Zeigegerät arbeitet, bis sie von einem speziellem Muster ak-



So sieht die Maus einen Matrix-Code auf einem Mauspad. Durch Filterung und Fehlerkorrektur gewinnt sie die IP-Adresse.

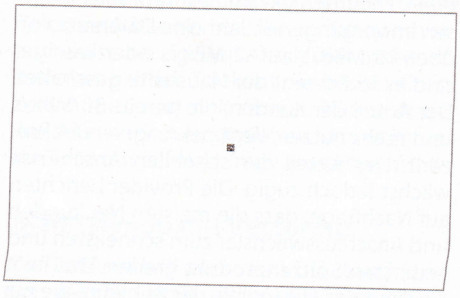


Der Eintrag im Gerätemanager deutet darauf hin, dass eine Schläfermaus aktiviert wurde.

tiviert wird. Anders als mit zusätzlicher Elektronik ausgestattete Mäuse sieht man diesen Varianten die Manipulation nicht an. Selbst wenn ein Sicherheitsbeauftragter die Maus aufschraubt und benutzt, wird er nichts Verdächtigtes entdecken und sie guten Gewissens freigeben. Erst in Kombination mit dem Mauspad funktioniert der Angriff. Dazu wurde die Firmware der Maus manipuliert, die die Minifotos nach bekannten Mustern durchsucht und gegebenenfalls in die Rolle einer Tastatur schlüpft, um Befehle zu senden.

Spurensuche

Mit einem Stereomikroskop begaben wir uns auf die Suche und fanden auf etlichen Mausunterlagen die vermuteten Muster. Anders als zunächst angenommen handelte es sich nicht um QR-Codes – diese würden relativ viele Pixel benötigen und ihre eckigen Muster sie möglicherweise für besonders scharfsichtige Zeitgenossen mit bloßem Auge leichter auffindbar machen. Vielmehr ist ein kleinerer und unregelmäßig aussehender Matrix-Code der Auslöser für die plötzlichen Mausaktivitäten. Doch die Codes aktivieren nicht nur die Spionagetätigkeit der Maus, in ihnen steckt zudem die IP-Adresse, die die Maus zusammen mit dem FTP-Befehl an den Rechner sendet. Pro Mauspad fanden sich im Schnitt 25 miniaturisierte Matrix-Codes zur Aktivierung und 25 weitere mit IP-Adressen, die neben den aufgedruckten Bildmotiven für das normale Auge kaum zu erkennen sind. Pro Pad war immer dieselbe IP-Adresse kodiert; unter den Pads variierten die IP-Adressen zwar, jedoch führten sie allesamt in Netze chinesischer Anbieter.



Mit diesem harmlosen Aktivierungscode in Miniaturausführung testen Sie, ob Sie eine Schläfermaus benutzen.

Wo wir die manipulierte Maus herhatten, können wir nicht mehr nachvollziehen. Genauer nachvollziehbar ist jedoch die Herkunft der präparierten Mauspads. Kollegen hatten sie als Give-aways an den Ständen ausländischer Aussteller auf der CeBIT 2013 erhalten. Wie die Angreifer eine Firmware mit Schadcode in der Maus installiert haben, ist bislang unklar. In den offiziellen Datenblättern des Sensor-Herstellers gibt es dazu keine Hinweise. Wir haben beim Bundesamt für Sicherheit in der Informationstechnik nachgefragt, ob Berichte über ähnliche Angriffe auf Industrie und Wirtschaft in Deutschland vorliegen. Dokumentiert ist jedoch nur ein Fall eines Rechtsanwalts, bei dem eine Maus zum Diebstahl der Mandantendatenbank zwecks späterer Erpressung Einsatz fand. Im Inneren fand ein Landeskriminalamt nach einer Analyse ein Teensy-Mikrocontroller-Board [2].

Selbsttest

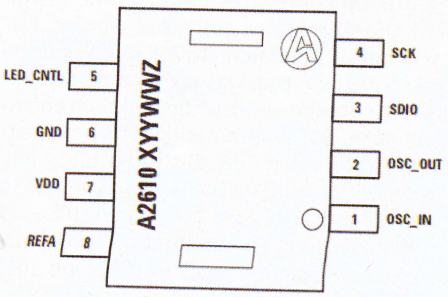
Um weiteren Schläfermäusen auf die Spur zu kommen, haben wir den harmlosen Aktivierungscode extrahiert und für Sie abgedruckt. Bewegen Sie Ihre Maus über das nebenstehende Bild und prüfen Sie anschließend im *Gerätemanager von Windows (Systemsteuerung/Hardware und Sound/Geräte und Drucker)*, ob dort unter „Tastatur" der Eintrag „HID-Tastatur" zu finden ist. Wenn ja, ist die Schläfermaus erwacht und hat sich als Human Interception Device im System eingenistet. Jetzt wartet sie darauf, IP-Adressen vom Mauspad einzulesen. Immerhin konnten wir auf diesem Weg zwei weitere Mäuse mit maliziösen Absichten in der Redaktion enttarnen.

Falls Ihre Maus betroffen ist, müssen Sie sie allerdings nicht entsorgen. Zwar gibt es nach unseren Recherchen keine Firmware-Updates, um die Maus zu desinfizieren. Solange man mit ihr jedoch keine Codes mit IP-Adressen einliest, passiert nichts. Allerdings müssen Sie künftig streng auf ihre Mauspad-Hygiene achten: Untersuchen Sie Ihre Unterlage mit einer Lupe, ob Codes aufgedruckt sind und drehen Sie sie gegebenenfalls um. Wenn Sie das Bild mögen, können Sie auch Pergamentpapier darüber legen, das macht die Codes für die Maus unlesbar. Sofern Ihr System schon vor dem Test den Eintrag im Gerätemanager zeigt, sollten Sie mit einem Virenscanner prüfen, ob die Maus bereits Schadcode nachgeladen hat. (dab)

Literatur

[1] Daniel Bachfeld, Angriff mit trojanischer Maus, c't 16/11, S. 44

[2] Video zur Netzwerkattacke: www.it-sicherheit.de/ratgeber/videos/lka_videos/netzwerkattacke/



Der Maussensor hat eine synchrone serielle Schnittstelle, über die er mit der Außenwelt kommuniziert. c't