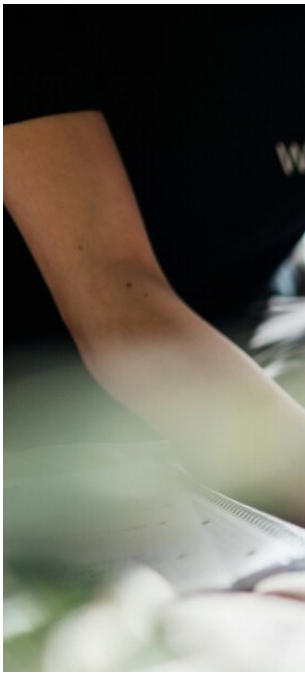
مستشعر الضوء في هاتفك يمكنه التجسس عليك دون تشغيل الكاميرا!



اكتشف باحثون من معهد ماساتشوستس للتكنولوجيا الجانب المظلم لأجهزة استشعار الضوء في الهواتف الذكية، والتي يمكن أن تساعد المتسللين على تتبع تحركات المستخدم.

وتقوم هذه المستشعرات الصغيرة بضبط سطوع شاشتك بناء على الضوء المحيط. ولكن على عكس الكاميرات، لا تحتاج التطبيقات إلى إذن منك للوصول إليها.

وكما اكتشف باحثو معهد ماساتشوستس للتكنولوجيا، فإن هذه الميزة التي تبدو بريئة لها جانب مظلم، حيث يمكن للقراصنة استغلال هذه المستشعرات لإعادة بناء صور لما يحدث أمام شاشتك مباشرة.

واكتشف الباحثون في مختبر علوم الكمبيوتر والذكاء الاصطناعي (CSAIL) التابع لمعهد ماساتشوستس للتكنولوجيا (MIT) أن هذا المستشعر يمكنه أيضا التقاط صور لإيماءات يدك والكشف عن خصوصيتك.

وللحصول على فهم أفضل، تخيل هذا الموقف: أنت تتصفح موقع ويب، غير مدرك تماما أن كل تمريرة تقوم

بها يتم التقاطها، ليس بواسطة الكاميرا، ولكن بواسطة مستشعر الضوء. أو أنت تشاهد فيلما مع صديق، وتضع يدك بشكل عرضي بالقرب من الشاشة، فمن الممكن أن يقوم أحد المتسللين بتجميع تفاعلاتك من بعيد.

ونشر الباحثون ورقة بحثية في مجلة "Advances Science" في وقت سابق من الشهر الجاري، تقترح خوارزمية تصوير حسابية يمكنها استعادة صورة البيئة من منظور شاشة العرض باستخدام تغييرات طفيفة في شدة الضوء التي يكتشفها المستشعر.

وقام فريق معهد ماساتشوستس للتكنولوجيا، بقيادة يانغ ليو، بتطوير خوارزمية تحلل التغيرات الدقيقة في شدة الضوء التي يلتقطها المستشعر عندما تلمس الأشياء الشاشة.

وتقوم الخوارزمية بإعادة بناء الصور المنقطة عن طريق تجميع هذه التقلبات معا، والكشف عن الإيماءات مثل التمرير والانتقال السريع.

ويقول المؤلف الرئيسي يانغ ليو، من قسم الهندسة الكهربائية وعلوم الكمبيوتر (EECS) وكالب الدكتوراه في مختبر علوم الكمبيوتر والذكاء الاصطناعي: "يعتقد الكثيرون أن هذه المستشعرات يجب أن تكون قيد التشغيل دائما".

وأظهر الفريق كيف يمكن للمتسللين استخدام هذه الخوارزمية للتجسس على إيماءات اليد، مثل التمرير أو الانتقال السريع، واستنتاج كيفية تفاعلك مع هاتفك أثناء مشاهدة مقاطع الفيديو.

فعلى سبيل المثال، يمكن للتطبيقات التي يمكنها الوصول إلى شاشتك، مثل مشغلات الفيديو ومتصفحات الويب، استخدام هذه التقنية لجمع بياناتك من دون إذن.

كيف اختبر الباحثون تهديد خصوصية التصوير هذا؟
قام الباحثون بتطبيق عملية التمرير على ثلاث عروض توضيحية باستخدام جهاز لوحي يعمل بنظام أندرويد.

وفي الاختبار الأول، قاموا بوضع دمية أمام الجهاز بينما كانت أيدي مختلفة تلامس الشاشة. وأشارت يد بشرية إلى الشاشة، وبعد ذلك، لامست الشاشة قطعة من الورق المقوى. وكشف فريق معهد ماساتشوستس للتكنولوجيا عن التفاعلات الجسدية مع الشاشة في الوقت الفعلي اعتمادا على مستشعر الضوء.

وفي اختبار ثان، أظهروا أن المتسللين يمكنهم تدريجيا التقاط كيفية قيام المستخدمين بالتمرير، والانتقال السريع، والضغط، وغيرها من خلال مستشعر ضوء أقوى والذي مكنهم من متابعة الحركات بمعدل إطار واحد كل 3.3 دقيقة.

ومن خلال مستشعر الإضاءة المحيطة الأسرع، يمكن للجهات الخبيثة التجسس على تفاعلات المستخدم في الوقت الفعلي مع جهازه.

ووجد اختبار ثالث أن المستخدمين معرضون للخطر أيضا عند مشاهدة مقاطع الفيديو مثل الأفلام والمقاطع القصيرة. وكانت يد بشرية تحوم أمام المستشعر أثناء عرض مشاهد من فيلم توم وجيري على الشاشة، مع وجود لوحة بيضاء خلف المستخدم تعكس الضوء على الجهاز. ومع ذلك، التقط مستشعر الإضاءة المحيطة التغيرات الدقيقة في الكثافة لكل إطار فيديو، مع إظهار الصور الناتجة لإيماءات اللمس.

وقال البروفيسور فيليكس هايد من جامعة برينستون: "يحول هذا العمل مستشعر الإضاءة المحيطة وشاشة جهازك إلى كاميرا"، مسلطا الضوء على مدى انتشار هذه الثغرة الأمنية على نطاق واسع وطبيعتها الخبيثة.

ويؤكد كذلك: "على هذا النحو، يسلط الباحثون الضوء على تهديد الخصوصية الذي يؤثر على فئة شاملة من الأجهزة تم التغاضي عنه حتى الآن".

وفي حين أثارت كاميرات الهواتف مخاوف تتعلق بالخصوصية لسنوات، فإن مستشعر الإضاءة المحيطة يمثل تحديا فريدا. فهو لا يتجاوز عمليات التحقق من الأذونات فحسب، بل إن طبيعته السلبية تجعله غير قابل للاكتشاف فعليا. ومن الممكن أن تقوم ببث أفعالك عن غير قصد إلى أحد المتسللين حتى مع تغطية الكاميرا.

ويقترح الباحثون إجراءين مضادين حاسمين:
- أذونات التطبيقات التفصيلية: يجب أن يكون لدى المستخدمين تحكم واضح في التطبيقات التي يمكنها الوصول إلى مستشعر الإضاءة المحيطة، وتمكينهم من تحديد من يمكنه إلقاء نظرة خاطفة على حياتهم الرقمية.

- خفض مستوى المستشعر: يؤدي الحد من دقة المستشعر وسرعته إلى تقليل المعلومات التي يجمعها، ما

يجعل من الصعب على المتسللين جمع بيانات ذات معنى.