Investigadores descubrieron un medio potencial para perfilar y rastrear a los usuarios en línea utilizando un enfoque novedoso que combina identificadores de dispositivos con su información biométrica.

Los detalles provienen de una investigación recientemente publicada titulada *«Nowhere to Hide: fuga de identidad intermodal entre biometría y dispositivos»*, realizada por un grupo de académicos de la Universidad de Liverpool, la Universidad de Nueva York, la Universidad China de Hong Kong y la Universidad de Buffalo Sol.

> *«Los estudios previos sobre el robo de identidad solo consideran el objetivo del ataque para un solo tipo de identidad, ya sea para identificaciones de dispositivos o biometría. Sin embargo, la parte que falta es explorar la viabilidad de comprometer los dos tipos de identidades simultáneamente y comprender profundamente su correlación en entornos IoT multimodales»,* dijo Chris Xiaoxuan Lu, profesor asistente de la Universidad de Liverpool.

Los investigadores presentaron los hallazgos en la Conferencia Web 2020 celebrada en Taipei la semana pasada. Se puede acceder al prototipo y al código asociado.

El mecanismo de fuga de identidad se basa en la idea de espionaje subrepticio de individuos en espacios ciberfísicos durante largos períodos de tiempo.

En pocas palabras, la idea es que un mal actor puede explotar la singularidad de la información biométrica de los individuos (rostros, voces, etc.) y las direcciones MAC de WiFi de los teléfonos inteligentes y dispositivos IoT para identificar de forma automática a las personas dibujando una correlación espacio-temporal entre los dos conjuntos de observaciones.

> *«El atacante puede ser incluso compañeros de trabajo que comparten la misma oficina con las víctimas o personas ajenas que usan sus computadoras portátiles para espiar a las víctimas al azar en una cafetería. Por lo tanto, lanzar un ataque de este tipo no es difícil, considerando que los dispositivos IoT multimodales son muy pequeños y se pueden disfrazar bien, como una cámara espía con función de detección de WiFi. En general, hay poco esfuerzo de configuración al costado del dispositivo agresor»,* dijo Xiaoxuan.

Para montar el ataque, los investigadores ensamblaron un prototipo de espionaje construido sobre una Raspberry Pi que consistía en una grabadora de audio, una cámara de 8MP y un sniffer WiFi que puede capturar los identificadores del dispositivo.

Los datos recopilados de esta forma no solo determinaron que existe una similitud de asistencia a la sesión entre la biometría física de uno y su dispositivo personal, sino que también son lo suficientemente únicos para poder aislar a un individuo específico entre distintas personas ubicadas en el mismo espacio.

Sin embargo, la precisión del ataque puede disminuir en caso de que una víctima esté oculta en una multitud y comparta el mismo patrón de asistencia a la sesión o muy similar con otro sujeto en él, algo que es difícil de suceder y poco práctico, según los investigadores.

Posibles técnicas de mitigación

Con miles de millones de dispositivos IoT conectados a Internet, los investigadores afirman que el efecto compuesto de dicha fuga de datos es una amenaza real, con el adversario capaz de desanonimizar más del 70% de los identificadores del dispositivo.

Ofuscar las comunicaciones inalámbricas y buscar micrófonos o cámaras ocultas podría ayudar a mitigar el ataque intermodal, aunque advierten que aún no existe una buena contramedida.

> *«Evite conectar WiFi a redes inalámbricas públicas, ya que deja expuesta su dirección MAC de WiFi subyacente. No permite que sus dispositivos IoT multimodales (como timbres inteligentes o asistentes de voz) lo supervisen las 24 horas, los 7 días a la semana, ya que envían datos a terceros sin transparencia para usted, y pueden ser pirateados fácilmente y pueden comprometer su ID en distintas dimensiones»,* dijo Xiaoxuan Lu.