الأمن الحيوي.. أنواعه ومستقبله

ابتكر الناس منذ القدم وسائل وطرق مختلفة لحفظ أوراقهم وأغراضهم الثمينة من أعين المتطفلين أو من أيدي السُرّاق، وفي كل مرة يُطوّر فيها اللصوص أساليبهم لكسر الأقفال، يلجأ الناس إلى تحسين طرق دفاعاتهم، واستمر الصراع إلى يومنا هذا ولا يوجد ما يشير إلى توقفه في يوم من الأيام.

ومن الطرق الحديثة المتداولة بين أيدي الجميع وضع كلمة مرور لحواسيبهم وهواتفهم المحمولة، بل وحتى لدخولهم إلى بعض الأماكن، فكانت كلمات المرور في البدء عبارة عن أرقام فقط، ثم أصبحت مزيجًا من الأرقام والحروف، فما لبث قراصنة الاختراق الإلكتروني حتى أوجدوا برمجيات تتيح لهم التسلل إلى داخل هذه الأنظمة المحمية.

يكاد لا يمر أسبوع إلا وتتعرض إحدى الشركات لاختراق بياناتها مسببةً بذلك سرقة معلومات عن الآلاف من روادها أو مستخدمي منتجاتها، ناهيك عن الخسائر المادية الناتجة عن ذلك الاختراق.

نتيجة لتكرار عمليات القرصنة وتطوير "الهاكرز" أساليبهم في الاحتيال، بدأت الكثير من الدول وكبرى شركات التكنولوجيا في البحث عن وسائل أنجع لحفظ أمن معلوماتهم، ومن هنا كانت الهجرة الجماعية نحو أنظمة "الأمن الحيوي" أو ما يطلق عليه أيضًا "القياسات الحيوية"

سوء اختيار بعض مستخدمي الإنترنت واستخفافهم بأهمية قوة كلمة السر الخاصة بهم، جعلهم صيدًا سهلًا للمتسللين، حيث كشف تقرير أجراه المركز القومي لأمن الإنترنت في المملكة المتحدة (NCSC) الحسابات التي كانت عرضة للاختراق، حيث تبين أن نحو 23 مليون مستخدم في المملكة المتحدة وحدها استخدم التسلسل "123456" ككلمة سر!

نتيجة لتكرار عمليات القرصنة وتطوير "الهاكرز" أساليبهم في الاحتيال، بدأت الكثير من الدول وكبرى شركات

التكنولوجيا في البحث عن وسائل أنجع لحفظ أمن معلوماتهم، ومن هنا كانت الهجرة الجماعية نحو أنظمة "الأمن الحيوي" أو ما يطلق عليه أيضًا "القياسات الحيوية".

ما القياسات الحيوية؟

القياسات الحيوية ببساطة هي أي مقاييس متعلقة بالسمات البشرية، وهي آلية أمنية تستخدم للمصادقة وتوفير الوصول إلى منشأة أو نظام معين بناءً على التحقق التلقائي والفوري من الخصائص المادية للفرد، ونظرًا لأن الأمن الحيوي يقيم العناصر الجسدية للفرد أو بياناته البيولوجية، فهو يعد من أقوى تقنيات الأمان المادي المستخدمة للتحقق من الهوية.

ومن الأمثلة الأكثر شيوعًا لنظام القياسات الحيوية هو تقنية التعرف على بصمات الأصابع والوجه لأجهزة الجوال الذكية المستخدمة حاليًا.

تخزن الأنظمة أو المحركات التي تعتمد على الأمن الحيوي خصائص جسم الإنسان التي لا تتغير على مدى حياة الفرد وتشمل بصمات الأصابع والملمس والصوت وأنماط اليد والتعرف على الوجه وقزحية العين

يتم تطبيق الأمن الحيوي بشكل أساسي في البيئات ذات متطلبات الأمان المادي الحرجة أو المعرضة بدرجة كبيرة لسرقة الهوية، حيث تخزن الأنظمة أو المحركات التي تعتمد على الأمن الحيوي خصائص جسم الإنسان التي لا تتغير على مدى حياة الفرد، وتشمل بصمات الأصابع والملمس والصوت وأنماط اليد والتعرف على الوجه وقزحية العين.

متى تم استخدام القياسات الحيوية لأول مرة؟

الاعتماد على القياسات الحيوية طريقة موغلة في القدم، إذ أظهرت الوثائق التاريخية أن الإمبراطور الصيني "تسان لي" أول من اعتمد على بصمة الأصبع في توثيق القرارات، أما في العهد القريب فكان بداية استخدامها في المملكة المتحدة من شرطة العاصمة لتحديد الهوية عام 1901، تلتها الولايات المتحدة عام 1902 من شرطة نيويورك وبعدها مكتب التحقيقات الفيدرالي عام 1924.

وعلى عكس كلمات المرور أو غيرها من وسائل الحماية، لا يمكن نسيان البيانات البيومترية أو تبادلها أو سرقتها وكذلك لا يمكن تزويرها، فوفقًا للحسابات التي أجراها السير فرانسيس غالتون (ابن عم داروين)، فإن احتمال العثور على بصمتين متشابهتين هو واحد من بين 64 مليار احتمال.

يتكون النظام الحيوي من ثلاثة مكونات مختلفة:

1- أجهزة الاستشعار: وهي التي تسجل المعلومات التعريفية الخاصة بالمستخدم.

2- الحواسيب: سواء كنت تستخدم معلوماتك الحيوية للوصول إلى جهاز كمبيوتر أم أي شيء آخر، يجب أن يكون هناك جهاز كمبيوتر يخزن المعلومات للمقارنة.

3- البرمجيات: البرنامج هو في الأساس ما يربط أجهزة الكمبيوتر بجهاز الاستشعار.

كيف تعمل القياسات الحيوية؟

عندما يتم تسجيل الفرد في نظام الأمان البيومتري، يلتقط المستشعر المحدد نقاط عديدة من على سطح الجزء المراد اعتماده كمرجع للحماية، على سبيل المثال، تعمل تقنية التعرف على الوجه في جهاز لمصادقة المستخدم وجه على الحمراء تحت نقطة 30000 عرض على Apple من iPhone X المستخدم من خلال مطابقة الأنماط.

القوالب المسجلة لكل مستخدم هي تمثيل رياضي (خوارزمية)، لا يمكن إعادة تصميم الخوارزمية أو إعادة إنشائها لذا لا يمكن تزويرها

ويقوم المستشعر باعتماد هذه النقاط كنقاط دلالة يبني عليها ما يسمى بخوارزمية توقيع أو قالب حيوي.

القوالب المسجلة لكل مستخدم هي تمثيل رياضي (خوارزمية)، لا يمكن إعادة تصميم الخوارزمية أو إعادة إنشائها لذا لا يمكن تزويرها، ويتم تخزين القالب للمقارنة المستقبلية في قاعدة بيانات مركزية، وعندما يكون التعرف على الهوية مطلوبًا، يقرأ القارئ خصائص الفرد في كل عملية مسح جديدة، وتتم مقارنة ميزات التعريف من القارئ بالقالب المخزن لتحديد إذا كان هناك تطابق.

أنواع الحمايات الحيوية المتوافرة اليوم

توجد أنواع عديدة لتقنيات الأمن الحيوي منها ما هو مستخدم الآن وقسم آخر يتم العمل على تطويره، وهي:

1- تقنية التعرف على اليد

تعتمد على قياس وتسجيل الطول والسمك والعرض ومساحة سطح يد الشخص، يرجع تاريخ هذه الأجهزة إلى الثمانينيات من القرن الماضي وكانت تستخدم عادة في تطبيقات الأمان.

"كلمة مرور الدماغ" أو "أفكاري هي كلمة المرور": هي قراءة رقمية لنشاط الدماغ عندما ينظر إلى مجموعة من الصور

2- تقنية مسح بصمة الأصبع

يلتقط نمط فريد من التلال والوديان على الأصبع، تستخدم العديد من الهواتف الذكية وبعض أجهزة الكمبيوتر المحمولة هذه التقنية كنوع من كلمة المرور لإلغاء قفل الشاشة.

3- تقنية التعرف على قزحية العين

يحدد الأنماط الفريدة لقزحية الشخص، وهي المنطقة الملونة للعين المحيطة بالبؤبؤ، وعلى الرغم من استخدامه على نطاق واسع في تطبيقات الأمان، فإنه لا يستخدم عادة في السوق الاستهلاكية.

4- تقنية التعرف على الصوت

يقيس موجات الصوت الفريدة في صوت المستخدم خلال التحدث إلى الجهاز، قد يستخدمها البنك الخاص بك للتحقق من هويتك عند الاتصال بحسابك، أو يمكنك استخدامه عند إعطاء تعليمات إلى مكبر صوت ذكي مثل Amazon's Alexa.

5- تقنية التعرف على السلوك

يحلل الطريقة التي تتفاعل بها مع نظام محوسب، يمكن لضغط المفاتيح والكتابة اليدوية وطريقة المشي وكيفية استخدام الماوس والحركات الأخرى تقييم هويتك ومدى معرفتك بالمعلومات التي تدخلها.

6- تقنية التعرف على الوجه

تقيس الأنماط الفريدة لوجه الشخص من خلال مقارنة وتحليل ملامح الوجه، يتم استخدامها في الأمن وتطبيق القانون ولكن أيضًا كوسيلة لمصادقة الهوية وإلغاء قفل الأجهزة مثل الهواتف الذكية وأجهزة الكمبيوتر المحمولة.

أنواع من القياسات الحيوية يتم تطويرها:

1- تقنية التعرف على الأفكار

"كلمة مرور الدماغ" أو "أفكاري هي كلمة المرور": هي قراءة رقمية لنشاط الدماغ عندما ينظر إلى

مجموعة من الصور، فعندما ينظر شخص ما إلى مجموعة من الصور أو يسمع مقطوعة موسيقية، يتفاعل دماغه ويستجيب بطريقة تُمكّن الباحثين من قياسها عن طريق مستشعرات مصمّمة لهذا الغرض.

يطمح المصممون إلى استخدام هذه الطريقة في حماية السيارات من السرقة، من خلال عرض مجموعة من الصور على الشاشة أمام السائق ويتأكدون من هويته من خلال تفاعل دماغه

لاحظ الباحثون من جامعتي بافولا وكولورادو في نيويورك أن استجابة كل إنسان تختلف تمامًا عن أي إنسان آخر أمام الصور نفسها، وتكون هذه الاستجابة ثابتة في الدماغ عند كل مرة يشاهد فيها الصور نفسها، وكذلك تكون لا إرادية، بحيث لا يتمكن الشخص من التحكم فيها.

هذه الاستجابة أو التفاعل هو ما يسميه العلماء "كلمة مرور الدماغ"، وسوف تعتمد هذه الطريقة من أساليب الحماية في المؤسسات والشركات التي تتطلب درجة أمان عالية.

ويطمح المصممون إلى استخدام هذه الطريقة في حماية السيارات من السرقة، من خلال عرض مجموعة من الصور على الشاشة أمام السائق ويتأكدون من هويته من خلال تفاعل دماغه، بعد ذلك تُرسل إشارة إلى محرك السيارة تسمح له بالعمل.

2- تقنية التعرف على المستخدم عبر الأذن

لقد توصل باحثون من جامعة نيويورك إلى تقنية جديدة تسمى EarEcho، وهي أداة القياس الحيوي الجديدة الخاصة بهم، تستخدم الموجات الصوتية لتحديد المستخدمين بناءً على الهندسة الفريدة للقناة الصوتية.

من خلال تحليل المعلومات الصوتية للصوت الذي تم تشغيله والصدى الذي تم التقاطه، الذي يرتبط ارتباطًا كبيرًا بهندسة قناة الأذن

أخذ الفريق زوجًا من سماعات الأذن الجاهزة ثم أضافوا لها ميكروفونًا يواجه قناة الأذن، وعندما يتم تشغيل الصوت بواسطة مكبر صوت السماعة في أذن المستخدم، ينتشر الصوت عبر قناة الأذن وينعكس مرة أخرى على الميكروفون المدمج في السماعة.

من خلال تحليل المعلومات الصوتية للصوت الذي تم تشغيله والصدى الذي تم التقاطه، الذي يرتبط ارتباطًا كبيرًا بهندسة قناة الأذن، يستخرج الباحثون الميزات الفريدة من المستخدم ومن ثم التحقق من هوية المستخدم.

لقد اتضح أيضًا أنه حساس بشكل مثير للإعجاب، مع نموذج أولي لجهاز EarEcho قادر على تحديد هوية المستخدمين بأكثر من 95% من الدقة.

هل تعبر القياسات الحيوية آمنة؟

بالنظر إلى أن خروقات البيانات أصبحت جزءًا لا مفر منه في عالمنا الرقمي، فهذا يعني أن الأمن الحيوي ليس له مستقبل طويل الأجل قبل أن يتم اختراقه أيضًا، فرغم استحالة تزويرها أو سرقتها لكن اختراقها لا يأتي منها بل من قواعد البيانات الخازنة لها.

وهذا بحد ذاته يعتبر نقطة ضعف قاهرة بحقها، فإذا تم اختراق هذه القواعد وتم سرقة القياسات الحيوية فليس بالإمكان إعادة تعيينها من جديد، إذ ليس بإمكان الشخص إبدال بصمة أصابعه أو تغيير وجهه أو قزحية عينه.

من المهم حقًا حماية بياناتنا الحيوية من التسرب إلى الأطراف غير المرغوب فيها، ولكن هذه ستصبح مهمة صعبة على نحو متزايد

فعلى سبيل المثال، عام 2015، تم اختراق قاعدة بيانات شيفرات حيوية لنحو 5.6 ملايين موظف فيدرالي أمريكي، قاد هذا الاختراق إلى عدم تمكّن هؤلاء من استخدام بصماتهم لتأمين أي جهاز شخصي، أو للعمل، لأن ما سيحتويه الجهاز سيتم اختراقه.

هذا يعني أنه من المهم حقًا حماية بياناتنا الحيوية من التسرب إلى الأطراف غير المرغوب فيها، ولكن هذه ستصبح مهمة صعبة على نحو متزايد ونحن نكشف بياناتنا البيومترية لمقدمي المزيد من الخدمات يوميًا.

رابط المقال: https://www.noonpost.com/29711/