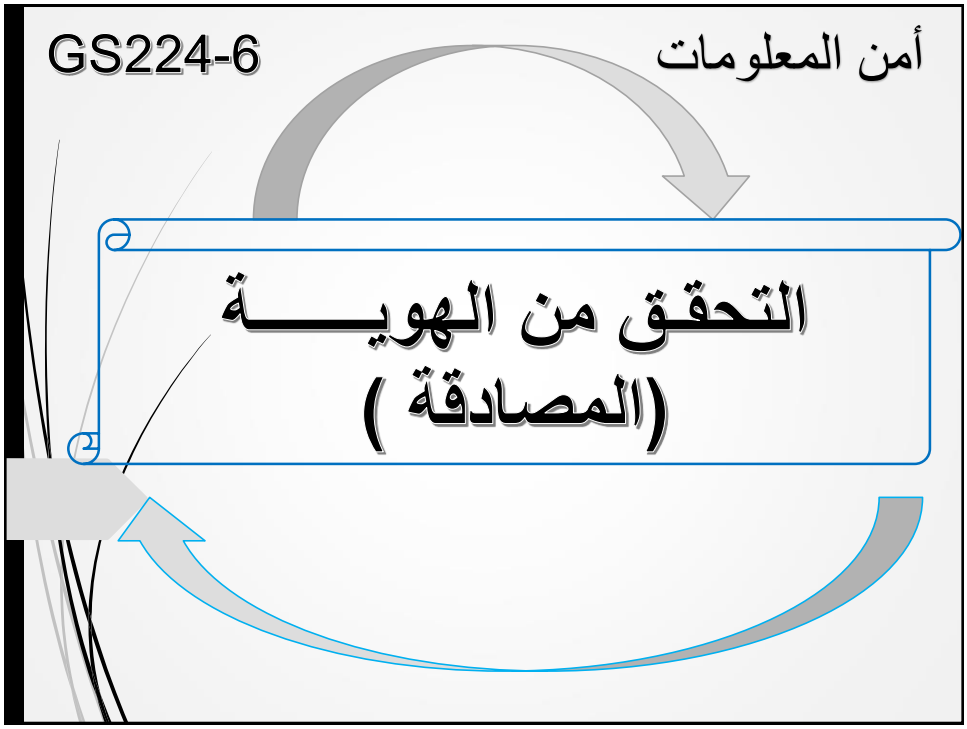



## التحقق من الهوية

في شبكات الحاسب الآلي، المصادقة هي العملية التي يقوم فيها المستخدم بإثبات أنه المالك للهوية التي يتم استخدامها. فعندما يقوم المستخدم بإدخال اسم المستخدم فإنه يحاول استخدام هوية للوصول إلى النظام. وللمصادقة على مستخدم (أي التحقق أن المستخدم هو في الواقع صاحب الهوية) فإن الخطوة التالية الأكثر شيوعاً هي أن نسأل عن بيانات الاعتماد. بيانات الاعتماد هي جزء (أو أجزاء) من المعلومات المستخدمة في التحقق من هوية المستخدم.

يعتبر التحقق من الهوية (المصادقة) هو اللبنة الأساسية للأمن وخط الدفاع الأول. (أساس التحكم في الوصول ومحاسبة المستخدم)

**"عملية التحقق من الهوية المدعى بها كيان ما للنظام أو لصالحه"**

- تتكون عملية المصادقة من خطوتين:
  - **التعريف**: تقديم المعرف لنظام الأمان. (يجب تعيين المعرف بعناية ، لأن الهويات المصادق عليها هي أساس خدمات الأمان الأخرى ، مثل خدمة التحكم في الوصول)
  - **التحقق:** تقديم أو إنشاء معلومات المصادقة التي تؤكد الارتباط بين الكيان والمعرف.
- **المعرف** هو الوسيلة التي يقدم المستخدم من خلالها هويته المزعومة للنظام ؛ **مصادقة المستخدم** هي وسيلة إثبات صحة الادعاء. لاحظ أن مصادقة المستخدم تختلف عن مصادقة الرسائل (عندما تهتم الأطراف المتصلة بسلامة تبادل الرسائل).

## التحقق من الهوية

خذ بعين الاعتبار هذا السيناريو: يعمل أحمد في قاعدة عسكرية محلية. بعد ظهر كل يوم، يتوقف في صالة الألعاب الرياضية بالقاعدة لممارسة التمارين. بعد أن أغلق أحمد سيارته بالمفتاح اللاسلكي، دخل إلى النادي وتعرف عليه سالم، موظف الاستعلامات بالنادي. يهنئ سالم أحمد لفوزه في المسابقة الأخيرة لقيامه بأكبر عدد من تمارين الضغط في دقيقة واحدة. ثم سمح له بالدخول إلى غرفة تغيير الملابس. بمجرد دخوله إلى غرفة تغيير الملابس، يفتح أحمد القفل الرقمي لخزانة ملابسه بسلسلة الأرقام التي يحفظها. أثناء ممارسته للتمرين، توجه المتدرب "محمود" إلى أحمد وقال: "كنت أعرف أنك أنت الذي يقوم بتمارين الضغط هذه على الرغم من أنني لم أتمكن من رؤية وجهك، لا أحد يمكنه فعل عدد أكبر، تهانينا بالفوز باللقب."

في هذا السيناريو، تم إثبات أن أحمد حقيقي أو أصيل، وليس دجالًا او منتحل، من خلال خمسة عناصر منفصلة. هذه موضحة في الشكل التالي:

## التحقق من الهوية

- **ماهو الموقع** : نظرًا لأن القاعدة العسكرية محاطة بسياج وحراس وبوابة مؤمنة، فلن تتم الموافقة على دخول المنتحل شخصية أحمد إلى القاعدة. وهذا يعني أن موقع أحمد يمكن أن يساعد في إثبات شخصيته.
- **ماذا يملك** : من خلال قفل أبواب سيارته بمفتاح السيارة اللاسلكي، وهو عنصر لا يملكه إلا أحمد الحقيقي، فما لديه يساعد على إثبات هويته.
- **من هو**: الوصول إلى غرفة تغيير الملابس محمي بشكل وهيئة جسد أحمد. يتعين على سالم أن يتعرف على خصائص جسده الفريدة (لون شعره، ووجهه، وشكل جسمه، وصوته، وما إلى ذلك) قبل أن يُسمح له بدخول غرفة تغيير الملابس، لذا تعمل هذه الخصائص على تأكيد هويته.
- **ماذا يعرف** : محتويات خزانة أحمد محمية بما يعرفه فقط أحمد الحقيقي، وهو تركيبة القفل. لن يُفتح القفل من قبل المحتال، بل فقط من قبل أحمد الحقيقي الذي يعرف تسلسل تركيبة الارقام.
- **ماذا يفعل** : نظرًا لأن أحمد هو الوحيد القادر على القيام بالعدد القياسي من تمارين الضغط، فإن ما يفعله يساعد في إثبات هويته بشكل فريد.

القفل التركيبي ( ماذا يعرف )

المفتاح اللاسلكي (ماذا يملك)

خصائص الوجه ( من هو )

تمرين الضغط (ماذا يفعل)

قاعدة عسكرية (ماهو الموقع)

## وسائل التحقق من المستخدم

ثلاث وسائل لمصادقة هوية المستخدم ، والتي يمكن استخدامها بمفردها أو مجتمعة: أساسها هو شيء الشخص :

- **يعرفه** ، على سبيل المثال كلمة المرور ، رقم التعريف الشخصي (PIN).
- **يمتلكه** ، على سبيل المثال البطاقات الذكية والمفتاح المادي .
- **منك** ، وهى القياسات الحيوية لجسم المستخدم، واساسها هو شيء الشخص:
  - **يجسده** (القياسات الحيوية الثابتة) ، على سبيل المثال التعرف على بصمات الأصابع وشبكية العين والوجه.
  - **يقوم به** (القياسات الحيوية المتغيرة) ، على سبيل المثال التعرف عن طريق الصوت والتوقيع وإيقاع الكتابة.

- يمكن استخدامها بمفردها أو مجتمعة لتحقيق هوية المستخدم.
- كل طريقة لديها مشاكل. قد يتمكن الخصم من تخمين كلمة المرور أو سرقتها. قد يكون الخصم قادرًا على تزوير أو سرقة البطاقة. قد ينسى المستخدم كلمة مرور أو يفقد رمزًا مميزًا. علاوة على ذلك ، هناك عبء إداري كبير لإدارة كلمات المرور ومعلومات البطاقات على الأنظمة وتأمينها في الأنظمة. مع المصادقات بالقياسات الحيوية (البيومترية) ، هناك مجموعة متنوعة من المشاكل ، بما في ذلك التعامل مع الإيجابيات الزائفة والسلبيات الكاذبة، وتقبل المستخدم لها ، والتكلفة ، والراحة.

## تقييم اخطار التحقق من المستخدم

- **مستوى التأكيد**: درجة اليقين من أن المستخدم قد قدم بيانات اعتماد تشير إلى هويته المدعية:
  - المستوى-1: ثقة قليلة (منتدى عبر الإنترنت)
  - المستوى-2: بعض الثقة (المنظمات المهنية)
  - المستوى-3: ثقة عالية (المتقدمون بمكتب براءات الاختراع)
  - المستوى-4: ثقة عالية جدًا (الموظفون يتعاملون مع خدمات خطيرة/حساسة)

- **التأثير المحتمل**: منخفض ، متوسط ، كبير .

## 1- التحقق من الهوية : كلمة المرور (شيء تعرفه)

كلمة المرور هي أقدم وأبسط شكل من أشكال بيانات المصادقة. وكلمة المرور هي سلسلة من الرموز السرية التي لا يعرفها سوى صاحب الهوية ويقوم باستخدامها للمصادقة على الهوية. فإذا قام الشخص الذي يحاول الوصول إلى الحساب بتقديم كلمة المرور الصحيحة فإنه يفرض أن هذا الشخص هو صاحب الهوية ويتم منحه الوصول. وتستخدم كلمات المرور على نطاق واسع لأنها لا تحتاج إلى أجهزة ولا تحتاج إلى برمجيات لتطبيقها. وعموما فهي الطريقة للتحقق من المستخدم المنتشرة على نطاق واسع :

- يقدم المستخدم الاسم/معرف الدخول وكلمة المرور
- يقارن النظام كلمة المرور بتلك المحفوظة لتسجيل الدخول المحدد

- مصادقة معرف تسجيل المستخدم وأن المستخدم مصرح له بالدخول إلى النظام ويحدد صلاحيات المستخدم، ومقدار التحكم بالوصول.
- نظام كلمة المرور يعتبر خط الدفاع الأمامي ضد المتسللين. جميع الأنظمة المتعددة المستخدمين تطلب من المستخدم ألا يقدم اسمًا أو معرفًا فحسب ، بل كلمة مرور أيضًا. يقارن النظام كلمة المرور بكلمة المرور المخزنة مسبقًا لمعرف هذا المستخدم ، والمحفوظة في ملف كلمات المرور في النظام. تعمل كلمة المرور على مصادقة معرف تسجيل الدخول الفردي إلى النظام. بدوره ، يحدد المعرف ما إذا كان المستخدم مصرحًا له بالوصول إلى نظام ، والصلاحيات الممنوحة للمستخدم ، ويستخدم لتحديد ضوابط الوصول التقديرية.

## 1- نقاط ضعف كلمة المرور

على الرغم من أن استخدام كلمات المرور يعد الأكثر شيوعاً من بين بيانات المصادقة الأخرى، إلا أنه هناك العديد من المسائل المتعلقة بأمن كلمات المرور منها كلمات المرور الضعيفة. وأيضاً فإن : المهاجمين يستخدمون طرق شائعة لتخمين كلمات المرور.

- **هجوم القاموس** (Dictionary attacks) **:** تجريب الآلاف من كلمات المرور المحتملة وذلك من قواميس ضخمة لكلمات المرور والكلمات الشائعة و متغيراتها المحتملة من لغات متعددة، حيث قد يتجاوز متسلل ما عناصر التحكم في الوصول ويسرق ملف كلمات المرور في النظام ، ثم يقارن المهاجم القيم المختزلة لكلمة المرور مقابل قيم كلمات المرور من القاموس بعد اختزالها باستخدام كل قيم الاضافة المتاحة. (نوعين: النسخة المسبقة ، عيد الميلاد). إذا لم يتم العثور على تطابق ، فسيقوم برنامج الاختراق بمحاولة إجراء تغييرات على جميع الكلمات الموجودة في قاموس بكلمات المرور محتملة. تشمل هذه التغييرات تهجئة الكلمات إلى الوراء ، أو الأرقام الإضافية أو الأحرف الخاصة ، أو تسلسل الأحرف ،
- **هجوم القوة الغاشمة** (Brute-force attacks) : يستهدف المهاجم حسابًا معينًا ويدخل تخمينات لكلمة المرور حتى يتم اكتشاف كلمة المرور الصحيحة، ويتم بمزج الحروف و الأرقام و الرموز عشوائياً وتجريبها حتى يتم تخمين كلمة المرور، بحيث يتم تجريب كل الاحتمالات الممكنة من التركيبات. عند استخدام برمجيات هجمات القوة الغاشمة الالية على المستخدم ادخال معطيات التالية للبرنامج : طول كلمة المرور، فئة الابجدية ، اللغة ، التنسيق ، الاستثناء.
- **اختطاف محطة العمل :** ينتظر المهاجم محطة عمل نشطة الى حين تركها مفتوحة التسجيل (نشطة بدون وجود مستخدم).

## 1- نقاط ضعف كلمة المرور

- **استغلال استخدام كلمة مرور متعددة**: عندما تشترك أجهزة شبكة مختلفة في نفس كلمة المرور أو كلمة مرور متماثلة لمستخدم معين.
- **المراقبة الإلكترونية**: إذا تم إرسال كلمة مرور عبر شبكة لتسجيل الدخول إلى نظام بعيد ، فإنها تكون عرضة للتنصت.
- **الهندسة اجتماعية**: يمكن الكشف عن كلمات المرور من خلال هجمات الهندسة الاجتماعية واستغلال أخطاء المستخدم، بما في ذلك التصيد الاحتيالي وتصفح الكتف والتفتيش في سلة المهملات.
- **الالتقاط** : هناك عدة طرق يمكن استخدامها لالتقاط كلمات المرور. يمكن لبرنامج راصد لوحة المفاتيح الموجود على الحاسوب من التقاط كلمات المرور التي يتم إدخالها عن طريق لوحة المفاتيح. أثناء انتقال كلمات المرور، يمكن استخدام هجمات الرجل في المنتصف وهجوم الإعادة . يمكن لمحلل البروتوكول أيضًا التقاط عمليات الإرسال التي تحتوي على كلمات مرور.
- **إعادة الضبط**: إذا تمكن أحد المهاجمين من الوصول الفعلي إلى حاسوب المستخدم، فيمكنه مسح كلمة المرور الحالية وإعادة تعيينها من جديد. تتطلب برامج إعادة تعيين كلمة المرور إعادة تشغيل الحاسوب من محرك أقراص ضوئي أو محرك فلاش محمول (USB) ويحتوي عادةً على إصدار من نظام تشغيل مختلف إلى جانب برنامج إعادة تعيين كلمة المرور. على سبيل المثال، لإعادة تعيين كلمة المرور على حاسوب يعمل بنظام التشغيل ميكروسوفت ويندوز، سيتم استخدام محرك فلاش محمول (USB) يعمل بنظام التشغيل لينوكس (Linux) وبرنامج إعادة تعيين كلمة المرور.
- **تخمين كلمة المرور لمستخدم واحد:** يحاول المهاجم اكتساب معلومة حول صاحب الحساب وسياسات كلمة مرور النظام ويستخدم هذه المعلومة لتخمين كلمة المرور.

## 1- تكسير كلمة المرور

- **هجوم كلمة المرور الشائعة**: تأتي الأجهزة مصممة لتكون متصلة عادة من المصنع بكلمة مرور افتراضية. وينطبق هذا الكلام على بعض التطبيقات البرمجية وقواعد البيانات. وتشير هجمات بيانات الاعتماد الافتراضية إلى الحوادث التي يقوم فيها قراصنة الحاسب بالوصول إلى نظام أو إلى برنامج محمي بواسطة اسم مستخدم وكلمة مرور موحدة ومحددة مسبقاً (ومن ثم تكون معروفة على نطاق واسع).
- **جداول قوس قزح**. على الرغم من أن القوة الغاشمة وهجمات القاموس كانت في السابق الأدوات الأساسية التي يستخدمها المهاجمون لاختراق كلمات مرور المختزلة المسروقة، إلا أن المهاجمين استخدموا مؤخرًا جداول قوس قزح. تعمل جداول قوس قزح على تسهيل هجمات كلمات المرور عن طريق إنشاء مجموعة كبيرة من البيانات المُنشأة مسبقًا من كلمات المرور المختزلة. هناك خطوتان لاستخدام جدول قوس قزح. الأول هو إنشاء الجدول نفسه. بعد ذلك، يتم استخدام هذا الجدول لكسر كلمة المرور. جدول قوس قزح هو تمثيل مضغوط لكلمات مرور ذات علاقة مرتبطة وبشكلها الصريح ومرتبة في تسلسل (يسمى سلسلة). لإنشاء جدول قوس قزح، تبدأ كل سلسلة بكلمة مرور أولية يتم اختزالها بقيمة مضافة ثم إدخالها في دالة اختزال تنتج كلمة مرور نصية مختلفة. يتم تكرار هذه العملية لعدد محدد من الجولات. كل صف في جدول قوس قزح يشمل كلمة المرور الأولية وآخر قيمة مختزلة لكلمة المرور في السلسلة. يتطلب استخدام جدول قوس قزح لكسر كلمة المرور أيضًا خطوتين. أولاً، تتم اختزال كلمة المرور المراد كسرها واستخدامها بتنفيذ نفس الإجراءات المستخدمة لإنشاء الجدول الأولي. وينتج عن هذا كلمة المرور الأولية للسلسلة. ثم يتم تكرار العملية، بداية بكلمة المرور الأولية هذه حتى يتم العثور على الاختزال الأصلي. كلمة المرور المستخدمة في التكرار الأخير هي كلمة المرور المكسورة.

**هجمات جدول قوس قزح**: يُنشئ المهاجم قاموسًا كبيرًا لكلمات المرور المحتملة ، لكل كلمة مرور

- يولد المهاجم قيم مختزلة المرتبطة بكل قيمة مضافة ممكنة.
- والنتيجة هي جدول ضخم لقيم الاختزال يُعرف بجدول قوس قزح. على سبيل المثال يقوم جدول 1.4 جيجا بتكسير 99.9٪ من كلمات مرور "ويندوز" الأبجدية في 13.8 ثانية
- يمكن مواجهتها باستخدام قيمة مضافة كبيرة بدرجة كافية وطول : اختزال كبير بدرجة كافية.

## 1- الإجراءات المضادة لاختراقات كلمة المرور

تشمل الإجراءات المضادة للثغرات الأمنية ضوابط من أجل:

- منع الوصول غير المصرح به إلى ملف كلمة المرور،
- تدابير كشف التسلل لتحديد الاختراق ، وإعادة إصدار كلمات المرور بسرعة في حالة اختراق ملف كلمة المرور،
- آلية قفل الحساب التي تمنع الوصول إلى الحساب بعد عدد من محاولات تسجيل الدخول الفاشلة ،
- سياسات ضد استخدام كلمات المرور الشائعة واستخدام كلمات المرور يصعب تخمينها،
- التدريب و فرض سياسات كلمات المرور التي تجعل من الصعب تخمين كلمة المرور،
- تسجيل خروج من محطة العمل تلقائيًا بعد فترة من عدم النشاط ،
- سياسة تحظر نفس كلمة المرور أو كلمة مرور مشابهة على أجهزة شبكة معينة ؛ تشفير الاتصالات.

من المفيد دراسة / البحث عن نقاط ضعف كلمات المرور لان طريقة كلمات المرور تعتبر الاكثر انتشارا ولا تزال الأكثر كفاءة .

**نصائح لكلمات المرور الجيدة**: الطول ، التعقيد ، التغيير ، التنويع.

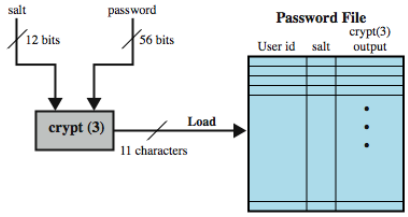
## 1- مستقبل كلمات المرور:

تم اقتراح العديد من آليات المصادقة لاستبدال كلمات المرور. وأحدى هذه الآليات آلية "تمرير وجه" (Pass faces) والتي يقوم فيها المستخدم بالاختيار المسبق لمجموعة من الوجوه البشرية، وأثناء محاولة تسجيل الدخول يقوم المستخدم باختيار أحد الوجوه من تلك المجموعة. وآلية أخرى هي آلية " النمط السرى" (draw –a-secret) والتي يقوم فيها المستخدم برسم خط متواصل عبر شبكة من المربعات. وبينما يكون من المرجح الاستمرار في استخدام كلمات المرور لفترة من الوقت، فإنه لن يكون من المستغرب أن تصبح هذه الآليات أو آليات مماثلة أكثر شعبية في السنوات المقبلة.

# 1- استخدام كلمات المرور المختزلة (Hashed passwords)

تحتفظ الحواسيب بكلمات المرور مختزلة بعد تحويلها بدوال الاختزال بدلاً من حفظ القيم الحقيقية لكلمات المرور. وبهذه الطريقة لا يمكن استرداد كلمات المرور حتى في حال سرقة الحاسوب، فإذا كانت كلمة المرور محفوظة كنص واضح فإن سرقة البيانات تؤدي إلى الحصول على كلمات المرور، ومن ثم فإن حفظ كلمة المرور مختزلة يساعد على حمايتها من السرقة. فعندما يقوم المستخدم بإدخال كلمة المرور الخاصة به، فإن الحاسوب يحسب دالة الاختزال لكلمة المرور ويقارنها مع دالة الاختزال المحفوظة في الحاسوب. فإذا تطابقت الاثنتان فإن الحاسوب يقبل كلمة المرور المدخلة وإلا فإنه يرفضها. وبهذه الطريقة فإن دوال الاختزال تسمح للحاسوب بالتحقق من كلمات المرور دون حفظ نسخة من كلمات المرور نفسها.

تقنية أمان لكلمة المرور المستخدمة على نطاق واسع هي استخدام كلمات المرور المختزلة والقيمة المضافة (salt value)، وتستخدم في نظام التشغيل يونيكس وغيره من أنظمة التشغيل الأخرى، والطريقة موضحة في الشكل (أ). لتحميل كلمة مرور جديدة في النظام ، يقوم المستخدم بتحديد كلمة مرور أو تعيينها. يتم دمج كلمة المرور هذه مع قيمة مضافة ذات طول ثابت (بحيث يمكن لكلمة مرور المستخدم نفسها إنشاء قيم مختزلة متعددة ، اعتمادًا على القيمة المضافة للمستخدم ، لجعل الهجمات أكثر صعوبة). في التطبيقات القديمة، ترتبط القيمة المضافة بالوقت الذي يتم فيه تعيين كلمة المرور للمستخدم. تستخدم التطبيقات الأحدث عددًا عشوائيًا . تعمل كلمة المرور والقيمة المضافة كمدخلات لخوارزمية الاختزال لإنتاج رمز اختزال ثابت الطول. تم تصميم خوارزمية الاختزال لتكون بطيئة في التنفيذ لإحباط الهجمات.



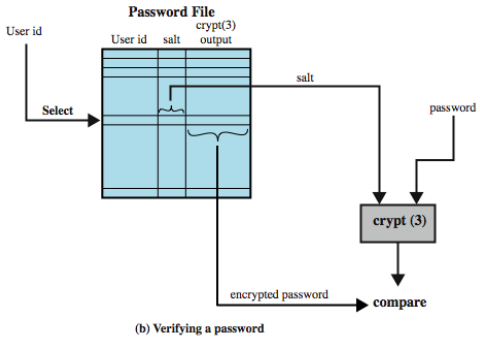

(a) Loading a new password

ثم يتم تخزين كلمة المرور المختزلة ، جنبًا إلى جنب مع نسخة نص عادي من القيمة المضافة ، في ملف كلمة المرور مقابل معرف المستخدم. لقد ثبت أن طريقة كلمة المرور المختزلة آمنة ضد مجموعة متنوعة من هجمات تحليل التشفير.

# 1- استخدام كلمات المرور المختزلة (Hashed passwords)

عندما يحاول المستخدم تسجيل الدخول إلى نظام ما ، يقدم المستخدم معرفًا وكلمة مرور (كما هو موضح في الشكل (ب)). يستخدم نظام التشغيل المعرف للفهرسة في ملف كلمات المرور واسترداد نص القيمة المضافة وكلمة المرور المشفرة. يتم استخدام كلمة المرور التي يدخلها المستخدم والقيمة المضافة كمدخلات في روتين التشفير. إذا تطابقات النتيجة مع القيمة المخزنة ، يتم قبول كلمة المرور. هناك نوعان من التهديدات لنظام كلمة المرور هذا:

- أولاً ، يمكن للمستخدم التمكن من جهاز باستخدام حساب ضيف
- أو من خلال بعض الوسائل الأخرى ثم تشغيل برنامج تخمين كلمة المرور يسمى برنامج تكسير كلمة المرور على هذا الجهاز




(b) Verifying a password

بالإضافة إلى ذلك ، إذا كان الخصم قادرًا على الحصول على نسخة من ملف كلمات المرور ، فيمكن تشغيل برنامج تكسير على جهاز آخر اثناء فراغه، ويتيح هذا للخصم تشغيل الملايين من كلمات المرور المحتملة في فترة زمنية معقولة.

## 1- لماذا القيمة المضافة (salt value)

- تمنع ظهور كلمات المرور مكررة في ملف كلمات المرور
- تزيد من صعوبة هجمات القاموس
- يكاد يكون من المستحيل معرفة ما إذا كان شخص ما يستخدم نفس كلمة المرور على أنظمة متعددة

## 1- كلمة المرور لمرة واحدة

كلمة المرور لمرة واحدة هي كلمة المرور التي يتم استخدامها مرة واحدة فقط. هذا النوع من كلمات المرور يجعل التنصت والتمليح عديم الفائدة. وتناقش هنا ثلاثة أساليب.

- الطريقة الأولى، يتفق المستخدم والنظام على قائمة كلمات المرور. يمكن استخدام كل كلمة مرور في القائمة مرة واحدة فقط. هناك بعض العيوب لهذا النهج. أولاً، يجب على النظام والمستخدم الاحتفاظ بقائمة طويلة من كلمات المرور. ثانيًا، إذا لم يستخدم المستخدم كلمات المرور بالتسلسل، فسيحتاج النظام إلى إجراء بحث طويل للعثور على المطابقة. هذا المخطط يجعل التنصت وإعادة استخدام كلمة المرور عديمة الفائدة. كلمة المرور صالحة مرة واحدة فقط ولا يمكن استخدامها مرة أخرى.
- الطريقة الثانية، يتفق المستخدم والنظام على تحديث كلمة المرور بشكل تسلسلي. يتفق المستخدم والنظام على كلمة المرور الأصلية، $P_1$، والتي تكون صالحة فقط للوصول الأول. أثناء الوصول الأول، يقوم المستخدم بإنشاء كلمة مرور جديدة، $P_2$، ويقوم بتشفير كلمة المرور هذه باستخدام $P_1$ كمفتاح . كلمة المرور للوصول الثاني هي $P_2$ . أثناء الوصول الثاني، يقوم المستخدم بإنشاء كلمة مرور جديدة، $P_3$، ويقوم بتشفيرها باستخدام $P_2$؛ يتم استخدام $P_3$ للوصول الثالث. بمعنى آخر، يتم استخدام $P_i$لإنشاء $P_{i+1}$ .بالطبع، إذا تمكنت المخترق من تخمين كلمة المرور الأولى ($P_1$)، فيمكن العثور على جميع كلمات المرور اللاحقة.
- الطريقة الثالثة، يقوم المستخدم والنظام بإنشاء كلمة مرور محدثة تسلسليًا باستخدام دالة التجزئة. في هذا الأسلوب، يتفق المستخدم والنظام على كلمة مرور أصلية، $P_0$، وعداد n . يقوم النظام بحساب $h^n (P_0)$، حيث يعني $h^n$ تطبيق دالة التجزئة h مرات.

## 1- توصيات إدارة كلمات المرور:

- تحديد سياسات لكلمات المرور ذات العلاقة باستخدام كلمات المرور. تحدد تلك السياسات نوع كلمات المرور المسموح بها (طولها ومدى تعقيدها). وبالنسبة لمسؤولي الأنظمة فإن سياسات كلمات المرور تحدد كيفية حفظ كلمات المرور، وكيفية إرسالها، وكيفية إصدارها للمستخدمين الجدد، وكيفية إعادة تعيينها إن لزم الأمر، كما يجب أن تأخذ في الاعتبار الأنظمة واللوائح الخاصة بالصناعة التي تعمل فيها المؤسسة.
- ضرورة الانتباه إلى التقنية المتبعة لحفظ كلمات المرور وذلك لتقليل من تخمين كلمات المرور وتكسيرها. فالوصول إلى الملفات وقواعد البيانات المستخدمة لحفظ كلمات المرور يجب أن يكون مقيداً بإحكام. وبدأ من حفظ كلمات المرور، ودالة اختزال كلمات المرور. ويجب أن تكون عملية تبادل كلمات المرور مشفرة حتى يستحيل قراءتها أثناء الإرسال. كما يجب التحقق بدقة من هوية جميع المستخدمين الذين يحاولون استعادة كلمات المرور المنسية أو إعادة تعيين كلمات المرور. وأخيراً يجب أن يكون كل مستخدم واعياً لمحاولات سرقة كلمات المرور من خلال هجمات الانتحال، أو من خلال استراق النظر من خلف المستخدم، أو غيرها من الطرق.
- لمنع تخمين وتكسير كلمات المرور، يجب أن تكون كلمات المرور معقدة بما فيه الكفاية، كما يتوجب غلق الحسابات التي تواجه العديد من محاولات تسجيل الدخول الفاشلة والمتعاقبة. وهذا يقلل من فرصة القراصنة في تخمين كلمات المرور. كما أن وضع قيود صارمة على الوصول لملفات كلمات المرور وقواعد البيانات التابعة لها يقلل من فرص تكسير كلمات المرور.
- ويحدد انتهاء صلاحية كلمة المرور المدة التي يمكن خلالها استخدام كلمة المرور قبل أن يكون مطلوباً من المستخدم أن يقوم بتغيرها حيث يقلل انتهاء صلاحية كلمة المرور من احتمالية استخدام كلمة المرور المخترقة بشكل مفيد. وعادة ما يتم جمع كلمات المرور من خلال إجراءات آلية، مما يسمح بوجود فاصل زمني بين جمع كلمات المرور وبين قيام المهاجم باستخدام كلمة المرور المخترقة. فإذا تم تغير كلمة المرور قبل محاولة المهاجم استخدامها، فإن كلمة المرور المخترقة لن تكون ضارة جداً. لكن انتهاء صلاحية كلمة المرور له بعض السلبيات خصوصاً إذا كانت المؤسسة تتطلب كلمات مرور مختلفة لأنظمتها المختلفة. المستخدم الذى ينسى كلمة المرور يحتاج إلى وحدة الدعم الفني، ذات التكلفة العالية، لاستعادة كلمة المرور المنسية. وبشكل عام يجب استخدام انتهاء صلاحية كلمة المرور بتعقل من خلال تطبيق فترات زمنية أطول للأنظمة التي تحتاج إلى قليل من الأمان.

## 1- نحو كلمة المرور افضل

- **مشاكل كلمات المرور** : يختار العديد من المستخدمين كلمة مرور قصيرة جدًا أو يسهل تخمينها. من ناحية أخرى ، إذا تم تعيين كلمات مرور للمستخدمين تتكون من ثمانية أحرف تم اختيارها عشوائيًا ، فإن اختراق كلمة المرور أمر مستحيل فعليًا، ولكن سيكون من المستحيل تقريبًا على معظم المستخدمين تذكر كلمات المرور الخاصة بهم.
- **الهدف**: هو القضاء على كلمات المرور التي يمكن تخمينها مع السماح للمستخدم بتحديد كلمة مرور يسهل تذكرها
- **التقنيات:**
  - **تعليم المستخدم**: يمكن إخبار المستخدمين بأهمية استخدام كلمات مرور يصعب تخمينها كما يمكن تزويدهم بإرشادات لاختيار كلمات مرور قوية. الإشكالية تحدث عندما يكون لديك عدد كبير من المستخدمين أو معدل تنقل المستخدمين كبير لأن العديد من المستخدمين سيتجاهلون الإرشادات ببساطة
  - **كلمات المرور منشأة من النظام**: لها تاريخ من ضعف القبول من قبل المستخدمين ، فإذا كانت عشوائية بطبيعتها فلن يتذكرها المستخدمون ، وإذا كانت منطوقة فقد يميل المستخدم إلى تدوينها.
  - **التحقق التفاعلي من كلمة المرور** (فحص دوري): حيث يقوم النظام بشكل دوري بتشغيل أداة تكسير كلمات المرور الخاصة به للعثور على كلمات مرور يمكن تخمينها. يقوم النظام بإلغاء أي كلمات مرور يتم تخمينها وإخطار المستخدم بذلك. إنجازها يمكن أن يكلف في الموارد.
  - **التحقق الاستباقي من كلمة المرور** (في وقت الانشاء): حيث يختار المستخدم كلمة المرور الخاصة التي يقوم النظام بعد ذلك بفحصها لمعرفة ما إذا كان مسموحًا بها ، وإذا لم يكن الأمر كذلك ، يرفضها. يجب أن يكون هناك توازن بين قبول المستخدم وقوة كلمة المرور. من المحتمل أن يكون هذا الحل هو الأفضل.

**مقياس عشوائية كلمة المرور (Password entropy):**

لسوء الحظ فإن تلك القواعد تولد كلمات مرور يصعب تذكرها، ولكن لا تؤدي بالضرورة إلى كلمات مرور قوية. ففي عام ٢٠٠٦ أصدر المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standard and Technology) منشوراً خاصاً (٨٠٠-٦٣)[٥] يُقدم تعريفاً حسابياً لقوة كلمة المرور اعتماداً على مقياس عشوائية (entropy)[٦] كلمة المرور. ويسمح لك مقياس العشوائية بمعرفة الوقت المستغرق للمهاجم لتخمين كلمة مرور معينة باستخدام هجمات القوة الغاشمة. على سبيل المثال، كلمة المرور التالية (d3nT1ty!) تُعد كلمة مرور قوية لأنها تلبي جميع القواعد النموذجية التي تم ذكرها أعلاه. واتضح أن كلمة المرور هذه تحتوي على ٢٥ بتاً من مقياس العشوائية والتي تمثل ٢٢٥ كلمة مرور محتملة (٣٣ مليون). وفي المتوسط فإن المهاجم يقوم بمحاولة أكثر من (١٦ مليون) كلمة مرور لتخمين القيمة الصحيحة. وبمعدل ١٠٠٠ محاولة في الثانية فإن المهاجم سيستغرق فقط ٤ ساعات لتخمين كلمة المرور. لكن عند استخدامك ٣-٤ كلمات شائعة، بدلاً من استخدام كلمة واحدة، باعتبارها عبارة المرور مثل «ورقة مقص حجر» تكون رفعت مقياس العشوائية إلى ٢٤١ والذي سيزيد من الوقت المطلوب لتخمين كلمة المرور إلى أكثر من ٨ سنوات.

وكما ترى فإن كلمة مرور ذات المقياس العشوائي العالي ستكون أكثر مقاومة لهجمات القوة الغاشمة[٧].

## 2- المصادقة القائمة على الادوات الرمزية (شيء تملكه)

القطع الرمزية (الأداة الرمزية): القطع الرمزية عبارة عن المكونات المادية (الادوات الرمزية البرمجية عبارة عن شفرة برمجية مخزنة في شيء مادي) التي يجب تقديمها لإثبات هوية المستخدم. وفي جميع الحالات تقريباً فإن الاداة الرمزية ترافق كلمات المرور("شيء تملكه" و "شيء تعرفه") مما يؤدي إلى إنشاء نظام مصادقة ثنائي. ويعد نظام المصادقة الثنائي وسيلة بسيطة نسبياً لإنشاء درجة عالية من الثقة لي هوية المستخدم الذي يحاول الوصول إلى النظام. وقد استخدمت المؤسسات المالية نظام المصادقة الثنائي (بطاقة الصراف الآلي والرقم السري) لعقود من الزمن، وكذلك الشركات الكبرى. لكن ومع زيادة حالات الانتحال الإلكتروني وغيرها من هجمات كلمات المرور في السنوات الأخيرة، توجهت العديد من المؤسسات لإضافة عامل إضافي لنظام المصادقة الحالي.

تسمى الاشياء التي يمتلكها المستخدم لغرض التحقق من المستخدم "الأدوات المميزة"، وتشمل هذه:

- **بطاقة منقوشة** :- أحرف مرفوعة في المقدمة ، على سبيل المثال بطاقة الائتمان القديمة
- **شريط مغناطيسي** :- شريط مغناطيسي في الخلف ، أحرف في المقدمة ، على سبيل المثال بطاقة مصرفية
- **قطع مميزة** :- أدوات الكترونية صغيرة كميدالية المفاتيح.
- **بطاقة ذاكرة** :- بها ذاكرة إلكترونية بداخلها ، على سبيل المثال بطاقة الهاتف مسبقة الدفع
- **البطاقة الذكية** :- بها ذاكرة إلكترونية ومعالج بالداخل ، على سبيل المثال بطاقة الهوية البيومترية (القياسات الحيوية) .
- **الهاتف المحمول** : يمكن إرسال الرمز إلى الهاتف الخليوي للمستخدم من خلال تطبيق على الجهاز أو كرسالة نصية عند استخدام كلمة المرور لمرو واحدة معتمدة في الوقت (TOTP) . وأيضًا يمكن للمستخدم بإرسال طلب عبر الهاتف لتلقي رمز التحقق .HOTP

## 2- بطاقة الذاكرة

- يمكن لبطاقات الذاكرة تخزين البيانات ولكن لا يمكنها معالجتها. تحتوي البطاقة الذكية على ذاكرة صغيرةُ تحفظ رمز المصادقة رقمياً يحدد المستخدم نفسه. أكثر هذه البطاقات شيوعًا هي البطاقة المصرفية التي تحتوي على شريط مغناطيسي على ظهرها.
- يمكن للشريط المغناطيسي تخزين رمز أمان بسيط فقط ، والذي يمكن قراءته (ولسوء الحظ إعادة برمجته) بواسطة قارئ بطاقات غير مكلف. كما توجد بطاقات ذاكرة تحتوي على ذاكرة إلكترونية داخلية.
- بطاقة ذاكرة إلكترونية قد تستخدم وحدها للوصول المادي (على سبيل المثال: غرف الفنادق) وبعضها يحتوي على كلمة مرور/ رقم تعريف شخصي (على سبيل المثال: أجهزة الصراف الآلي)
- توفر بطاقة الذاكرة ، عند دمجها مع رقم التعريف الشخصي أو كلمة المرور أمانًا أكبر بكثير من كلمة المرور وحدها. يجب أن يكتسب الخصم الحيازة المادية للبطاقة (أو أن يكون قادرًا على نسخها) بالإضافة إلى معرفة رمز التعريف الشخصي (التوثيق الرقمي). ويتم استخدام البطاقات الذكية في مجموعة واسعة من التطبيقات، بدءاً من بطاقات (SIM) الهاتفية داخل كل هاتف محمول وصولاً إلى بطاقات الوصول المستخدمة في الوصول المادي لتأمين مناطق المنشآت الحكومية والعسكرية. وبديلا للمصادقة المستندة إلى المصادقة المادية، يمكن تحميل شفرة المصادقة مباشرة في قرص يو إس بي (USB thumb drive) ، وتساعد الاداة الرمزية المِعتمدة على المصادقة باستخدام قرص يو إس بي (USB) على الاستغناء عن قارئ البطاقة الذكية كما تساعد على تأمين الحفظ الداخلي من خلال استخدام كل من المصادقة بالرمز البرامجي وكلمة المرور.

## 2- بطاقة الذاكرة

من بين العيوب المحتملة ما يلي:

- **يتطلب قارئًا خاصًا**: من عيوب الادة الرمزية المعتمدة على البطاقات الذكية، وكذلك من عيوب التوثيق باستخدام قرص يو إس بي أن المستخدم يجب أن يكون لديه وصول مادي لمنفذ يو إس بي أو يكون لديه قارئ بطاقة ذكية موصول بالنظام. يؤدي هذا إلى زيادة تكلفة استخدام الأداة المميزة ويخلق متطلبًا للحفاظ على أمان الأجهزة وبرمجيات القارئ. كما ان هذا ليس ممكناً دائماً خاصة عند استخدام الأجهزة المحمولة أو عند تسجيل الدخول من معمل حاسبات مفتوح الاستخدام أو مقهى لإنترنت.
- **فقدان القطعة المميزة**: تمنع الأداة الرمزية المفقودة صاحبها مؤقتًا من الوصول إلى النظام. وبالتالي هناك تكلفة إدارية لاستبدال الأداة المفقودة. بالإضافة إلى ذلك ، إذا تم العثور على الأداة الرمزية أو سرقتها أو تزويرها ، فلا يحتاج الخصم الآن إلا إلى تحديد رقم التعريف الشخصي للحصول على وصول غير مصرح به.

شكل (٨-٣): بطاقة ذكية في قارئ بطاقة متصل بمنفذ يو إس بي (USB)


- **استياء المستخدم**: على الرغم من أن المستخدمين قد لا يواجهون صعوبة في قبول استخدام بطاقة الذاكرة للوصول إلى أجهزة الصراف الآلي ، إلا أن استخدامها للوصول إلى الحاسوب قد يعتبر غير مريح.

## 2- القطع المميزة: كلمة المرور واحدة لكل تسجيل

وفي البيئات المفتوحة و العامة مثل استخدام الأجهزة المحمولة أو عند تسجيل الدخول من معمل حاسبات مفتوح الاستخدام أو مقهى لإنترنت، فإن الأداة الرمزية التي لا تحتاج إلى اتصال مباشر بجهاز الحاسب الآلي تكون مطلوبة. وبإمكان قطع مميزة بحجم سلسلة المفاتيح من شركة (RSA) مثلا التعامل مع هذه المشكلة من خلال توليد سلسلة من الأرقام التي يتم عرضها على شاشة (LCD) صغيرة في الجزء الأمامي من القطعة الرمزية. وبعد ذلك يتم إدخال سلسلة الأرقام من قبل المستخدم ككلمة مرور مرة واحدة (One-time password)، وهي عبارة عن كلمة المرور يمكن استخدامها مرة واحدةُ فقط وعادة تكون صالحة لفترة محدودة فقط. وتعد القطع المميزة التي من هذا القبيل شائعة الاستخدام منذ سنوات عديدة في القطاع الخاص والقطاع الحكومي لأنها سهلة التطبيق نسبياً، ولا تتطلب قارئاً خاصاً أو غيرها من الملحقات لتكون متصلة بكل جهاز حاسب آلي في المؤسسة، كما يمكن استخدامها بسهولة في أجهزة الحاسب الآلي المكتبية أو المحمولة.

الشكل (٨-٤): قطعة رمزية (Token)


## 2- القطع المميزة: كلمة المرور واحدة لكل تسجيل


وتقوم هذه الأنواع من القطع الرمزية باستحداث كلمة مرور مرة واحدة من خال أساليب تعتمد على الوقت أو أساليب تعتمد على الحدث.

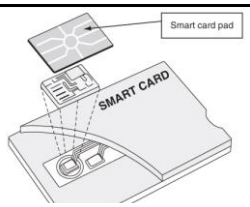
- تعمل القطع الرمزية التي تعتمد على الوقت على استحداث كلمة مرور جديدة خلال فترة زمنية محددة، تستمر عادة 30 أو 60 ثانية بواسطة خوارزمية معقدة تستحدث سلسلة من كلمات مرور لا يمكن تخمينها وهى مشتركة مع النظام المراد الوصول اليه.
- أما القطع الرمزية التي تعتمد على الحدث فتستخدم خوارزميات معقدة لاستحداث كلمة مرور لا يمكن تخمينهاً بناء على حدث معين تم إدخاله و ليس الوقت.

وبغض النظر عن النوع المستخدم، يتم تسجيل القطعة الرمزية في خادم المصادقة قبل أن ُتعطى للمستخدم، مما يؤدي إلى إعطائها قيمة مبدئية لبدء خوارزمية تعتمد على الحدث أو إلى مزامنة الساعة الداخلية لبدء الأسلوب المِعتمد على التسلسل.

وبالإضافة إلى القطع الرمزية فإن موردي الأجهزة الأمنية مثل شركة (RSA) تقدم قطع رمزية برمجية (software tokens)، وهي عبارة عن تطبيقات للهاتف المحمول تعمل بنفس طريقة القطع الرمزية لكن لا تتطلب من المستخدم أن يحمل جهاز منفصل. وأنها لا تنطوي على تقديم جهاز فعلي فإن هذه القطع الرمزية البرمجية لها فائدة إضافية تتمثل في الانتشار السريع والبسيط – من خلال تثبيت التطبيق. ومجرد تثبيت التطبيق فإن القطع الرمزية البرمجية تعمل تماماً مثل القطع الرمزية المادية المتنوعة - يقوم التطبيق بتوليد كلمة مرور تستخدم مرة واحدة، والتي يمكن بعد ذلك دمجها مع كلمة مرور المستخدمُ لتحقيق مصادقة النظام. وتعد أداة مصادقة جوجل (Google Authenticator) قطعة رمزية برمجية للمصادقة الثنائية لحسابات جوجل، وذلك في الهواتف الذكية التي تعمل بنظام الآي أو إس (OS) او نظام الأندرويد (Android).

## 2- القطع المميزة: كلمة المرور واحدة لكل تسجيل

- وبالإضافة إلى تطبيقات القطع الرمزية البرمجية فإن القدرات المميزة لأجهزة المحمولة الحديثة زادت من عدد الخيارات المتاحة للمصادقة الثنائية . فالرسائل النصية القصيرة (SMS) تعد طريقة مبسطة لتوفير عامل إضافي للمصادقة حيث يقوم المستخدمون أثناء إعداد حساباتهم بتسجيل أرقام هواتفهم المحمولة في خدمة المصادقة. وبعد ذلك عندما يحاول المستخدم المصادقة، يتم إرسال رمز المرور في رسالة قصيرة إلى هاتفه المحمول. ثم يقوم المستخدم بإدخال الرمز لإثبات أن الهاتف المحمول والمسجل مسبقاً لا يزال في حوزته. وأحد عيوب استخدام الرسائل القصيرة وسيلة لاعتماد بيانات المصادقة هو أن العديد من شركات الهاتف المحمول تأخذ رسوماً على كل رسالة.
- وتقدم شركة (tiQR) مثالاً عن نهج جديد للمصادقة وذلك بالاستفادة من الميزات الموجودة في الهواتف الذكية. فعند تسجيل الدخول إلى موقع محمي من شركة (tiQR)، يتم عرض عبارة مرور مشفرة للمستخدم على شكل رمز الاستجابة السريعة (Quick Response Code). وبعد ذلك يقوم المستخدم بأخذ صورة لرمز الاستجابة السريعة باستخدام تطبيق (tiQR) الموجود في الجهاز الذي للمستخدم ( وتطبيق (tiQR) متوفر على أجهزة أندرويد وأجهزة آي أو إس) حاليا. ثم يقوم المستخدم بإدخال كلمة المرور في تطبيق (tiQR) ويرسلها إلى خادم المصادقة مع عبارة المرور التي تم فك شفرتها. ويقوم خادم المصادقة بالتحقق من كلمة مرور المستخدم ومن عبارة المرور للتأكد من هوية المستخدم.



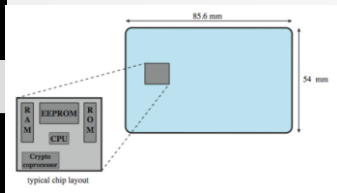

## 2- البطاقة الذكية

البطاقات الذكية فهي عبارة عن قطع رمزية في حجم البطاقة الائتمانية تقوم بحفظ رقم الهوية والذي يحدد البطاقة بشكل فريد، لها مظهر بطاقة الائتمان ، ولها واجهة إلكترونية، وقد تستخدم أيًا من بروتوكولات المصادقة الممكنة مع القارئ/الحاسوب باستخدام

- كلمة مرور ثابتة : تشبه بطاقات الذاكرة.
- ديناميكية : كلمات المرور التي يتم إنشاؤها كل دقيقة ؛ يتم إدخالها يدويًا عن طريق المستخدم أو إلكترونيًا
- استجابة التحدي : ينشئ الحاسوب رقمًا عشوائيًا ؛ توفر البطاقة الذكية التجزئة الخاصة بها (على غرار – التشفير بالمفتاح العام ).

- تحتوي البطاقة الذكية بداخلها على معالج دقيق كامل ، بما في ذلك المعالج والذاكرة ومنافذ الإدخال / الإخراج ، يتضمن بعضها دائرة معالجة مشتركة خاصة لعملية التشفير لتسريع مهمة تشفير الرسائل وفك تشفيرها أو إنشاء توقيعات رقمية للتحقق من صحة المعلومات المنقولة.
- في بعض البطاقات ، يمكن الوصول إلى منافذ الإدخال / الإخراج مباشرة بواسطة قارئ متوافق عن طريق تماسات اتصال كهربائية مباشرة. تعتمد البطاقات الأخرى بدلاً من ذلك على هوائي مضمن للاتصال اللاسلكي بالقارئ.

## 2- البطاقة الذكية




- تتضمن البطاقة الذكية النموذجية ثلاثة أنواع من الذاكرة.
  - تخزن ذاكرة القراءة فقط (ROM) البيانات التي لا تتغير خلال عمر البطاقة ، مثل رقم البطاقة واسم حامل البطاقة.
  - تحتوي ذاكرة القراءة فقط (EEPROM) القابلة للبرمجة وللمسح كهربائيًا على بيانات التطبيقات والبرامج ، مثل البروتوكولات التي يمكن للبطاقة تنفيذها وتحتوي أيضًا على بيانات قد تختلف بمرور الوقت.
  - تحتفظ ذاكرة الوصول العشوائي (RAM) بالبيانات المؤقتة التي يتم إنشاؤها عند تنفيذ التطبيقات.
- بديل البطاقة الذكية هو جهاز ذاكرة فلاش صغير وغير مكلف يُعرف باسم "دونجل فلاش" لها نفس وظيفة البطاقة الذكية ، ولكنها تتصل بمنفذ "USB" الموجود على الحاسوب ، وبالتالي فهي لا تحتاج إلى قارئ بطاقات معين.

## 2- بطاقة الهوية الالكترونية

- تطبيق هام للبطاقات الذكية "الهوية الإلكترونية الوطنية" (eID) ، وتخدم نفس الغرض مثل بطاقات الهوية الوطنية الأخرى (على سبيل المثال ، رخصة القيادة) ، ويمكن أن تقدم إثباتًا أقوى للهوية
  - البطاقة ألالمانية (بيانات مطبوعة على البطاقة):
    - البيانات الشخصية ( الاسم ، تاريخ الميلاد ، العنوان ، ... )، رقم الوثيقة (9- احرف ابجدية فريدة لكل بطاقة)، رقم الوصول إلى البطاقة (رقم عشوائي مكون من ستة أرقام: قد يستعمل ككلمة مرور) ، منطقة القراءة الآلية :نص من 3 اسطر(قد تستعمل ككلمة مرور)
    - الاستخدامات: (ePass) - الاستخدام الحكومي ، (eID) - الاستخدام العام ، (eSign) - يمكن أن يكون للمفتاح الخاص وشهادة مصادقة المفتاح .

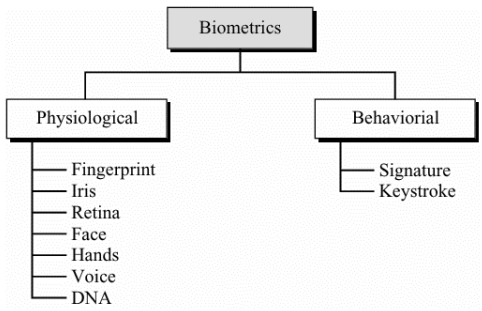
## 3- القياسات الحيوية : التحقق الحيوي (شيء منك)

تعد القطع الرمزية والقطع الرمزية البرمجية وسيلة رائعة لإضافة عامل إضافي لزيادة الأمن، ولكن مثل أي شيء مادي فإن القطع الرمزية يمكن أن تضيع أو تسرق ومن ثم تستخدم من قبل المهاجمين لانتحال شخصية المستخدمين. كيف يمكننا التأكد بأن الشخص الذي يحاول الوصول إلى النظام هو بالتأكيد الشخص صاحب الهوية؟ الأجهزة الحيوية تحلل الفروق الدقيقة لي بعض المواصفات الجسدية أو السلوكية، مثل بصمات الأصابع أو نمط الأوعية الدموية في العين، وذلك لتحديد هوية الفرد. وبشكل عام فإن الأجهزة الحيوية تعمل من خلال مقارنة بين بيانات القياسات الحيوية التي يتم أخذها من الشخص وبين نسخة من بيانات القياسات الحيوية للشخص والتي تم أخذها سابقاً أثناء عملية التسجيل. وإذا كانت بيانات القياسات الحيوية للشخص الذي يحاول الوصول إلى النظام تطابق البيانات المحفوظة في النظام، فإنه يفرض بأنه نفس الشخص وتكون عملية المصادقة ناجحة. ويطلق على الفروق المادية التي يمكن ملاحظتها بين الناس بالعلامات الحيوية. وهناك العديد من العلامات التي يمكن استخدامها، ولكن يتم تحديد مدى ملائمة العلامات من خلال العديد من العوامل، بما في ذلك:

- العمومية: يجب أن تكون السمة أو الصفة لدى كل شخص.
- التفرد: لا يوجد شخصان لهما الصفة نفسها.
- الدوام: يجب ألا تتغير الصفة مع مرور الوقت.
- التحصيل: يجب أن تكون الصفة قابلة للقياس كمياً.
- الأداء: يجب أن يتم الحصول على قياس دقيق من خلال موارد معقولة.
- القبول: استعداد المستخدمين لقبول قياس الصفة.
- التلاعب: صعوبة تقليد صفات شخص آخر.

## 3- القياسات الحيوية : التحقق الحيوي (شيء منك)

يحاول نظام المصادقة بالقياسات الحيوية التحقق من هوية الشخص بناءً على خصائصه الجسدية الفريدة ، والتي تشمل الخصائص الجسدية الثابتة: مثل بصمات الأصابع وملامح راحة اليد وخصائص الوجه وأنماط شبكية العين وقزحية العين ؛ والخصائص السلوكية المتغيرة : مثل البصمة الصوتية والتوقيع، (كما هو موضح بالشكل). بالمقارنة مع كلمات المرور والادوات المميزة ، تعتبر المصادقة بالقياسات الحيوية معقدة ومكلفة تقنيًا ، ولم تنضج بعد كأداة قياسية لمصادقة المستخدم على أنظمة الحاسوب. ويوضح الشكل التالي مؤشرًا تقريبيًا للتكلفة النسبية ودقة المقاييس الحيوية الأكثر شيوعًا.

## 3- القياسات الحيوية : تقنيات التحقق الحيوي

- **خصائص الوجه** (Face): تحديد الخصائص بناءً على الموقع النسبي وشكل ملامح الوجه الرئيسية ، مثل العينين والحاجبين والأنف والشفتين وشكل الذقن. وتقوم هذه التقنية بتحليل هندسة الوجه بناءً على المسافة بين ملامح الوجه مثل الأنف والفم والعينين. تجمع بعض التقنيات بين السمات الهندسية وملمس الجلد. تدعم كاميرات الفيديو القياسية وهذه التقنية كلاً من التحقق وتحديد الهوية. ومع ذلك، يمكن أن تتأثر الدقة بالنظارات ونمو شعر الوجه والشيخوخة.
- **ملامح اليد** (Hands) : تقيس هذه التقنية أبعاد اليدين، بما في ذلك شكل الأصابع وطولها وعرضها. يمكن استخدام هذه التقنية في المحيط الداخلي والخارجي. ومع ذلك، فهو أكثر ملاءمة للتحقق بدلاً من تحديد الهوية.
- **بصمات الأصابع** (Fingerprint): نمط النتوءات والأخاديد الموجودة على سطح الإصبع ، ويعتقد أنها فريدة من نوعها بين جميع البشر. تستخرج أنظمة بصمات الأصابع الآلية عددًا من الميزات لاستخدامها كبديل للنمط الكامل.
- **نمط شبكية العين** (Retina) : تقوم الأجهزة المخصصة لهذا الغرض بفحص الأوعية الدموية الموجودة في الجزء الخلفي من العين (أوردة تحت سطح الشبكية) الفريدة من نوعها، وبالتالي فهي مناسبة للتعرف على المستخدم. ويستخدم صورة رقمية لنمط الشبكية عن طريق عرض شعاع منخفض الكثافة من الضوء المرئي أو الأشعة تحت الحمراء على العين. ومع ذلك، فإن هذه الأجهزة باهظة الثمن وغير شائعة بعد.
- **القزحية** (Iris) : تقيس هذه التقنية النمط التفصيلي الموجود داخل القزحية والذي يكون فريدًا لكل شخص (سمة فيزيائية فريدة). وعادة ما يتطلب شعاع الليزر (الأشعة تحت الحمراء). فهي دقيقة للغاية ومستقرة على مدى حياة الشخص. كما أنها تدعم التحقق وتحديد الهوية. ومع ذلك، فإن بعض أمراض العيون، مثل إعتام عدسة العين، يمكن أن تغير نمط القزحية.

## 3- القياسات الحيوية : تقنيات التحقق الحيوي

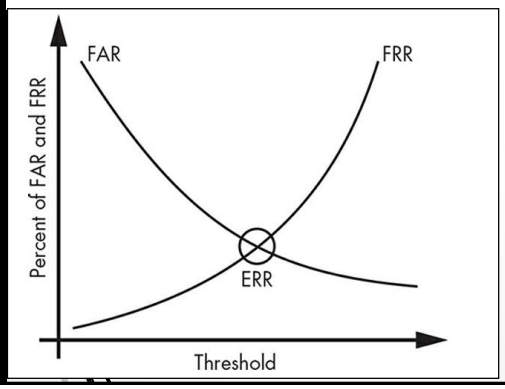
- **الصوت** (Voice): يقيس التعرف على الصوت طبقة الصوت والإيقاع ونبرة الصوت نتيجة ارتباطها بالخصائص الفيزيائية والتشريحية للمتحدث . يمكن استخدامه محليًا (ميكروفون) أو عن بعد (قناة صوتية). تستخدم هذه الطريقة في الغالب للتحقق. ومع ذلك، يمكن أن تتضاءل الدقة بسبب الضوضاء في الخلفية أو المرض أو العمر، مما يعقد مهمة التعرف على القياسات الحيوية.
- **الحمض النووي** (DNA) : وهو المادة الكيميائية الموجودة في نواة جميع خلايا الإنسان ومعظم الأعضاء الأخرى. ويستمر هذا النمط طوال الحياة وحتى بعد الموت. إنها دقيقة للغاية. يمكن استخدامه للتحقق وتحديد الهوية. المشكلة الوحيدة هي أن التوائم المتماثلة قد تشترك في نفس الحمض النووي.
- **نقر المفتاح** (Keystroke): تقيس تقنية نقرات المفاتيح (إيقاع الكتابة) سلوك الشخص المتعلق باستخدام لوحة المفاتيح. يمكنه قياس مدة الضغط على المفاتيح، والوقت بين نقرات مفاتيح، وعدد الأخطاء وتكرارها، ومقدار الضغط على المفاتيح، وما إلى ذلك. وهي غير مكلفة لأنها لا تتطلب معدات جديدة. ومع ذلك، فهي ليست دقيقة للغاية لأن السمة يمكن أن تتغير مع مرور الوقت (يصبح الناس أسرع أو أبطأ في الكتابة). كما أنها تعتمد على النص.
- **التوقيع** (Signature): لكل شخص أسلوب فريد في الكتابة اليدوية ، ولا سيما في التوقيع. تستخدم الأساليب القياسات الحيوية انماط التوقيع والأقلام الخاصة للتعرف على الشخص. لا تقوم هذه الأجهزة بمقارنة التوقيع فحسب، بل تقوم أيضًا بقياس بعض السمات السلوكية الأخرى، مثل التوقيت اللازم لكتابة التوقيع. تُستخدم التوقيعات في الغالب للتحقق.

## 3- القياسات الحيوية : الدقة و التطبيقات

يتم قياس دقة تقنيات القياسات الحيوية باستخدام معياريين: **معدل الرفض الزائف (FRR)** ، **ومعدل القبول الزائف (FAR)**.

**معدل الرفض الزائف** (FRR) : يقيس هذه المعيار عدد المرات التي لا يتعرف فيها النظام على الشخص الذي يجب التعرف عليه (الشرعي). يتم قياسه كنسبة الرفض الخاطئ إلى إجمالي عدد المحاولات (بالنسبة المئوية).

**ومعدل القبول الزائف** (FAR) : تقيس هذه المعيار عدد المرات التي يتعرف فيها النظام على الشخص الذي لا ينبغي التعرف عليه (المتسلل). يتم قياسه كنسبة القبول الخاطئ إلى إجمالي عدد المحاولات (بالنسبة المئوية).




نريد تجنب كلتا الحالتين، يجب أن تهدف إلى تحقيق التوازن بين الخطأين، ويشار إليه **بمعدل الخطأ المتساوي (EER)** . إذا قمت برسم كل من (FAR) و (FRR) على رسم بياني،(كما الشكل)، فإن (EER) يمثل النقطة التي يتقاطع فيها الخطان. نستخدم أحيانًا معدل (EER) كمقياس لدقة أنظمة القياسات الحيوية.

## 3- القياسات الحيوية : الدقة و التطبيقات

**التطبيقات** : توجد العديد من تطبيقات القياسات الحيوية قيد الاستخدام الفعلي. في البيئات التجارية، يشمل بوابات الدخول إلى المرافق، والوصول إلى أنظمة المعلومات، والمعاملات عند نقاط البيع، وضبط توقيتات الموظفين. وفي نظام إنفاذ القانون، تشمل التحقيقات (باستخدام بصمات الأصابع أو الحمض النووي) وتحليل الطب الشرعي. تستخدم مراقبة الحدود ومراقبة الهجرة أيضًا بعض التقنيات الحيوية.

## 3- القياسات الحيوية : التحقق البيومتري (بصمات الأصابع)

كانت تكنولوجيا مسح بصمات الأصابع شائعة الاستخدام فقط في التطبيقات التي تتطلب أماناً عالياً، لكن ومع انخفاض أسعار تكنولوجيا المسح وانخفاض تعقيدها أصبحت ماسحات بصمات الأصابع جزءاً من أجهزة الحواسيب المحمولة و الهواتف النقالة. وتعتمد ماسحات بصمات الأصابع إما على مجسات ضوئية في شكل كاميرا صغيرة تأخذ صوراً رقمية لإصبع، أو على ماسحات ضوئية بالسعة (capacitive scanners) والتي تولد صورة من إصبع المستخدم باستخدام التيار الكهربائي. وبدلاً من مقارنة كامل بصمة الإصبع، يقوم برنامج المسح الضوئي مقارنة شكل ومكان العديد من ميزات البصمة الفريدة (التفصيلات)، وعن طريق مطابقة التفصيلات بين بصمتي الأصابع، يستطيع البرنامج حساب احتمال تطابق البصمتين.


(٨-٥): بصمة الإصبع مع تحديد (تفصيلات) البصمة

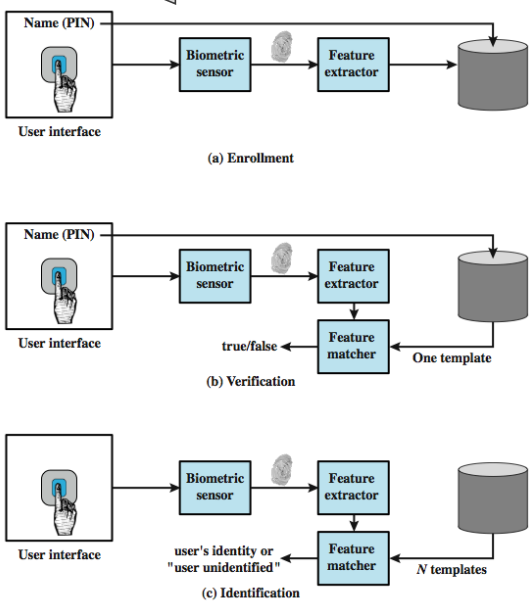
وهذا النوع من المطابقة الاحتمالية يمنع العوامل البيئية (الإضاءة، البقع الموجودة على الكاميرا، وغيرها) مُن التأثير على نتيجة تطابق بصمات الأصابع. ومع ذلك فإنها تعد نقطة ضعف في مصادقة القياسات الحيوية. ولا يحتاج المهاجم للحصول على تطابق تام للبصمة من أجل انتحال الشخص المستهدف بل يكفي أن يقوم المهاجم بنسخ ما يكفي من "التفصيلات" من أجل إقناع الماسح الضوئي بأنه الشخص الصحيح "المحتمل". وعلى الرغم من أنه تم نشر الهجمات الناجحة ضد ماسحات بصمات الأصابع إلا أنها ستظل التقنية الآمنة عموماً والتقنية الأكثر استخداماً في تحديد هوية القياسات الحيوية لسنوات قادمة.

## 3- كيفية استخدام التحقق بالقياسات الحيوية

يجب أولاً تسجيل كل شخص ليتم تضمينه في قاعدة بيانات المستخدمين المصرح لهم في النظام (مشابه لتخصيص كلمة مرور للمستخدم). بالنسبة لنظام المقاييس الحيوية ، يقدم المستخدم اسمًا ، وعادةً ما يكون نوعًا من كلمة المرور أو رقم تعريف شخصي للنظام. في نفس الوقت ، يستشعر النظام بعض الخصائص الحيوية لهذا المستخدم (مثل بصمة إصبع السبابة اليمنى). يقوم النظام برقمنة الإدخال ثم يستخرج مجموعة من الميزات التي يمكن تخزينها كرقم أو مجموعة من الأرقام التي تمثل هذه الخاصية الحيوية الفريدة ؛ ويشار إلى هذه المجموعة من الأرقام باسم "نموذج المستخدم". تم تسجيل المستخدم الآن في النظام ، والذي يحتفظ للمستخدم باسم معرف ، وربما رقم التعريف الشخصي أو كلمة المرور ، وقيمة المقاييس الحيوية. اعتمادًا على التطبيق ، تتضمن مصادقة المستخدم بنظام المقاييس الحيوية إما للتحقق أو لتحديد الهوية.

- يُعد **التحقق** مماثلاً لتسجيل دخول المستخدم إلى نظام ما باستخدام بطاقة ذاكرة أو بطاقة ذكية مقترنة بكلمة مرور أو رقم التعريف الشخصي . للتحقق من الهوية ، يقوم المستخدم بإدخال رقم التعريف الشخصي ويستخدم أيضًا مستشعر المقاييس الحيوية. يستخرج النظام الميزة المقابلة ويقارنها بالنموذج المخزن لهذا المستخدم. إذا كان هناك تطابق ، فإن النظام يصادق على هذا المستخدم.
- بالنسبة لنظام **تحديد الهوية** ، يستخدم الشخص مستشعر المقاييس الحيوية ولكنه لا يقدم معلومات إضافية. ثم يقارن النظام النموذج المقدم مع مجموعة النماذج المخزنة. إذا كان هناك تطابق ، فسيتم تحديد هوية هذا المستخدم. خلاف ذلك ، يتم رفض المستخدم.

## 3- كيفية عمل التحقق البيومتري (القياسات الحيوية)




**يوضح الشكل كيفية استخدام نظام القياسات الحيوية:**

- **التحقق** مماثل لتسجيل دخول المستخدم عبر البطاقة الذكية ورقم التعريف الشخصي
- **تحديد الهوية** هي معلومات قياسات حيوية ولكن بدون معرفات ؛ يقارن النظام مع القوالب المخزنة

## 4- المشاكل الأمنية لنظم مصادقة المستخدم

كما هو الحال مع أي خدمة أمن ، فإن التحقق من المستخدم ، ولا سيما التحقق من المستخدم البعيد ، يخضع لمجموعة متنوعة من الهجمات

- **هجمات العميل**: يحاول الخصم تحقيق مصادقة المستخدم دون الوصول إلى المضيف البعيد أو إلى التدخل في مسار الاتصالات
  - الخصم يحاول التنكر كمستخدم شرعي (على سبيل المثال في نظام قائم على كلمة المرور ، قد يحاول الخصم تخمين كلمة مرور المستخدم المحتملة).
  - الإجراء المضاد: كلمات مرور قوية ؛ الحد من عدد المحاولات.
- **هجمات المضيف**: يتم توجيه هجمات المضيف إلى ملف المستخدم في المضيف حيث يتم تخزين كلمات المرور أو رموز المرور المميزة أو نماذج المقاييس الحيوية
  - الإجراء المضاد: الاختزال وحماية قواعد بيانات كلمات المرور
- **التنصت**: يحاول المهاجم تعلم كلمات المرور من خلال مراقبة المستخدم ، والعثور على كلمات المرور المكتوبة ، وتسجيل نقرات المفاتيح وما إلى ذلك
  - التدابير المضادة الحرص على الاحتفاظ بكلمات المرور
  - مصادقة متعددة العوامل
  - مهمة المشرف: إبطال كلمات المرور المخترقة

## 4- المشاكل الأمنية لنظم مصادقة المستخدم

- **إعادة التشغيل**: تتضمن هجمات إعادة التشغيل خصمًا يكرر استجابة المستخدم التي تم التقاطها مسبقًا.
  - إجراء مضاد : بروتوكول الاستجابة للتحدي ، رموز المرور لمرة واحدة
- **حصان طروادة**: في هجوم حصان طروادة ، يتنكر تطبيق أو جهاز مادي كتطبيق أو جهاز أصلي بغرض التقاط كلمة مرور المستخدم أو رمز المرور أو المقاييس الحيوية. يمكن للخصم بعد ذلك استخدام المعلومات التي تم التقاطها للتنكر كمستخدم شرعي
  - الإجراء المضاد: مصادقة العميل ضمن بيئة أمنية موثوقة
- **منع الخدمة**: يحاول هجوم منع الخدمة تعطيل خدمة مصادقة المستخدم عن طريق إغراق الخدمة بمحاولات مصادقة عديدة.
  - الإجراء المضاد: مصادقة متعددة العوامل بأداة مميزة.

## 5- تسجيل الدخول الأحادي (Single sign-on):-

عند التحقق من هوية المستخدم فإنه يمنح حق الوصول إلى النظام أو التطبيق. وإذا كانت هذه المصادقة على الحساب المحلي، مثل تسجيل الدخول إلى نظام ويندوز على الحاسوب الشخصي، فإن عملية المصادقة تكون مكتملة. ويقوم نظام التشغيل بإعلام جميع البرامج في الحاسوب بهويتك ومن ثم لا حاجة للقيام بالمصادقة مرة أخرى. لكن ما الذي يحدث إذا كان التطبيق الذي تريد الوصول إليه موجوداً ُ على نظام آخر؟ كيف يمكنك أن تعرف نفسك إلى التطبيق البعيد؟ .

بإمكانك تكرار عملية المصادقة وتزويد النظام باسم المستخدم وكلمة المرور وأي عامل آخر (مثل القطع الرمزية، والقياسات الحيوية، وغيرها) المطلوبة في البيئة الخاصة بك. وهذا سيؤدي الغرض لكن سرعان ما يُصبح ذلك مملا خصوصاً إذا كنت ترغب في الوصول إلى العديد من الأنظمة. وما نحتاج إليه هو وسيلة تساعد على تسجيل الدخول مرةً ُ وحدة ومن ثم الوصول إلى جميع التطبيقات المتصلة دون المطالبة ببيانات المصادقة مرة أخرى. ويشار الى هذا النظام "تسجيل الدخول الأحادي" (single sign-on) (SSO) . ويقصد "تسجيل الدخول الأحادي" هو التقنية التي تسمح للمستخدم بتسجيل الدخول مرة واحدة ومن ثم الوصول إلى جميع الموارد المصرح للمستخدم الوصول إليها.

وعموماً فإن مسؤول النظام في بيئة "تسجيل الدخول الأحادي" يقوم بإنشاء كلمةَ مرور للمستخدم لكل مِورُد يسمح للمستخدم بالوصول إليه بحيث تكون كلمة المرور قوية وفريدة، كما يقوم مسؤول النظام بتغير كلمات المرور التابعة للموارد الفردية بشكل منتظم كما هو محدد من قبل سياسة كلمات المرور التابعة للمؤسسة. والمستخدم النهائي ليس على علم بأي من كلمات المرور التابعة للموارد الفردية. وبدلاً من ذلك يتم منح المستخدم كلمة مرور واحدة يقوم بإدخالها للوصول إلى الموارد التي يتم التحكم بها من خال تقنية "تسجيل الدخول الأحادي".

## 5- تسجيل الدخول الأحادي (Single sign-on):-

يتم تنفيذ تقنية "تسجيل الدخول الأحادي" عادة من خلال استخدام مستودع مركزي واحد للمصادقة المعتمدة على كلمات المرور. ومجرد قيام المستخدم بالمصادقة في هذا المستودع المركزي يقوم النظام بالبحث عن الموارد المصرح للمستخدم الوصول إليها. وعند محاول المستخدم الوصول لأي من هذه الموارد فإن نظام "تسجيل الدخول الأحادي" يعمل على توفير كلمة المرور الخاصة بالمورد نيابة عن المستخدم. وأصبح استخدام "تسجيل الدخول الأحادي" شائعاً بازدياد في المؤسسات الكبيرة مثل الجامعات والمصارف.

**مزايا وعيوب نظام تسجيل الدخول الأحادي**: هناك العديد من **الفوائد الرئيسية** التي يقوم "تسجيل الدخول الأحادي" بتوفيرها مباشرة لكل من المستخدمين ومسؤولي النظام:

1)تجربة أفضل للمستخدم: فلا أُحد يحب إدخال بيانات المصادقة عدة مرات.
2)تحفظ بيانات المصادقة بشكل سري: بحيث يكون المستخدم وخادم "تسجيل الدخول الأحادي" فقط لديهم إمكانية الوصول إلى بيانات المصادقة للمستخدم. وهذا ُيلغي إمكانية وصول المهاجم لكلمة المرُور من خلال خدمة مخترقة.
3)تنفيذ سهل للمصادقة الثنائية العوامل بدلاً من تحديث جميع الخدمات التي تدعم المصادقة من خلال القطع الرمزية وبيانات القياسات الحيوية، فإن نظام "تسجيل الدخول الأحادي" فقط يحتاج إلى التحديث.
4)أقل حيرة: لا يحتاج المستخدمون إلى تذكر حسابات متعددة بأسماء مستخدمين وكلمات مرور مختلفة.
5)اتصالات أقل لمكتب المساعدة الفنية: على الأغلب فإن المستخدمين سيتذكرون كلمات المرور التابعة لهم.
6)كلمات مرور قوية: بما ان المستخدم يحتاج لتذكر كلمة مرور واحدة فقط فإنه من الممكن أن تكون كلمة المرور أكثر تعقيداً.
7)تدقيق مركزي: يتم تأمين جميع المصادقات ويمكن رصدها في مكان واحد.

## 5- تسجيل الدخول الأحادي (Single sign-on):-

وبشكل عام فإن تطبيق تقنية "تسجيل الدخول الأحادي" تطور من مستوى الأمن ومن خبرة المستخدم، لكن هذه التقنية لا تخلو من **العيوب**:

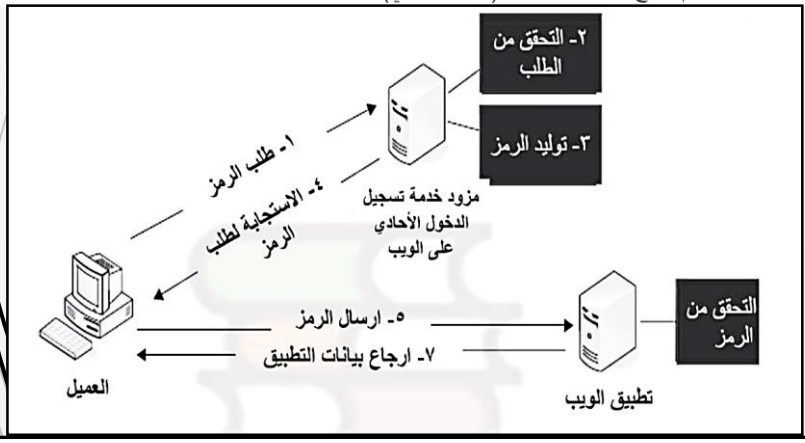
1) اختراق بيانات الاعتماد يمثل خطراً كبيراً - فاختراق حساب واحد يؤدي إلى الوصول إلى العديد من الأنظمة أو التطبيقات.
2) هجمات الانتحال - فوجود صفحة تسجيل واحدة تمثل هدفاً جذاباً للمخادعين حيث يستطيع هؤلاء المخادعون من نسخ لغة ترميز النصوص التشعبية (HTML) الخاصة بصفحة تسجيل الدخول التابعة لك مما يسهل سقوط المستخدمين في هذه الخدعة.
3) يمثل نظام "تسجيل الدخول الأحادي" نقطة الفشل الواحدة" (single point of failure) فإذا لم يكن هذا النظام متوفراً لا يمكن لأحد المصادقة على أي نظام. وتعطل المستودع سيؤدي لإضرار ليس فقط بخصوصية وتكامل جميع كلمات المرور في المستودع، بل سيضر أيضاً بجاهزية جميع الأنظمة التي يتحكم فيها هذا المستودع.
4) إضافة أي نوع من "تسجيل الدخول الأحادي" سيزيد من تعقيد النظام بأكمله. وكلما كان الحل أكثر تعقيداً، زادت احتمالية حدوث الأخطاء.

## 5- تسجيل الدخول الأحادي : التقنيات

- الدليل النشط و برتوكول كيربيروس
- المصادقة المعتمدة علي الرموز
- برتوكول خدمة المصادقة المركزية
- نظام الارتباط الاتحادي :
  - برتوكول لغة تمييز التأكيدات الأمنية
  - برتوكول (OpenID)

## 5- تسجيل الدخول الأحادي : المصادقة المعتمدة على الرموز

ابسط شكل من اشكال (تسجيل الدخول الأحادي على شبكة الانترنت) هو استخدام رمز مصادقة مشترك.
والمصادقة المعتمدة على الرمز المشترك هي استخدام مُعرف فريد او دالة تجزئة مشفرة تثبت هوية المستخدم بملكيته للرمز. فعندما يحاول المستخدم للمرة الأولى الوصول الى احد تطبيقات الشبكة المحمية، تتم إعادة توجيه المستخدم الى خدمة مزود الرموز للتحقق من اسم المستخدم و كلمة المرور (وأي معامل مصادقة أخر مطلوب)، وبعد ذلك يتم انتاج رمز المصادقة (الشكل التالي).



## 5- تسجيل الدخول الأحادي : المصادقة المعتمدة على الرموز

واعتماداً عـلى التنفيذ المحدد لتزويد الرمز فإن رمز المصادقة قد يُسـتحدث بعدد من الطرق المختلفة. والأكثر شـيوعاً أن الرمز ينتج من عملية تشفير مثل تمرير اسم المستخدم خلال خوارزمية دالة التجزئة الآمنة (HMAC-MD5) أو خوارزمية تشـفير المفتاح السري (AES). وبمجرد أن يتم توليد الرمز فإنه يتم إعادة توجيه المستخدم إلى الخدمة المطلوبة، كما يتم إضافة الرمز إلى معايير طلب بروتوكول انتقال النص التشـعبي (HTTP). وبديلاً لهـذه العملية يتم حفظ الرمز على شـكل ملـف تعريف الارتبـاط (cookie) في متصفح المسـتخدم قبل إعادة توجيه المسـتخدم إلى الخدمة المطلوبة. ويتم حفظ ملفات تعريف الارتباط التابعة للجلسة في الذاكرة المؤقتة فقط ويتم حذفها عندما يقوم المستخدم بإغلاق المتصفح. وبالإضافة إلى بيانات المصادقة يُمكن للتطبيقات أن تحفظ بيانات أخرى في ملفات تعريف الارتباط التابعة للجلسـة مثل العناصر المحفوظة في عربة التسـوق الإلكترونية أو تفضيلات الموقع للمستخدم.

وفي تطبيقات الشبكة فإن عملية التحقق من رمز المصادقة تعتمد على الطريقة المتبعة في توليد ذلك الرمز. وفي أبسط الحالات، إذا تم استخدام خوارزمية المفتاح المتماثل فإن تطبيق الشبكة المطلوب سيقوم بإدخال الرمز وإدخال نسخة من المفتاح المشفر إلى خوارزمية فك التشـفير. وتتضمن البيانات الناتجة في الحد الأدنى على اسـم المستخدم للشخص المُصادق، لكنها قد تتضمن بيانات أخرى عن الشخص مثل الاسم، أو بيانات المصادقة الأخرى كالختم الزمني وعنوان بروتوكول الإنترنت (IP).

ويعد «تسجيل الدخول الأحادي» باستخدام المصادقة المعتمدة على الرموز سهل التطبيق نسـبياً، كما يعد آمناً عندما يتم تنفيذه بالشـكل الصحيح باسـتخدام مفتاح تشـفير قوي. لكن هناك بعض المشـكلات. المشـكلة الأولى هي أنه لا يوجد بروتوكول أو نموذج موحد للمصادقة بالرموز، لذلك تقوم كل منظمة بتطبيق نظام المصادقة بشـكل مختلف. وهذه لا تُمثل مشكلة إذا كانت جميع التطبيقات التي ستستخدم «تسجيل الدخول الأحادي» تم تصميمها داخل المنظمة، لكن هذه النقطة تمثل مشـكلة كبيرة عند محاول دمج تطبيقات خارجية. والمشـكلة الأخرى تتمثل في صعوبة التعامل مع إدارة تشفير المفاتيح. فإذا قمت بتوليد مفتاح فريد لكل تطبيق يسـتخدم «تسـجيل الدخول الأحادي» فهناك احتمال أنك تحتاج إلى الإدارة مئات من المفاتيح. ومن جهة أخرى إذا استخدمت مفتاحاً واحداً لجميع الخدمات، وتم اختراق هذا المفتاح، فإن جميع الخدمات ستكون معرضة للخطر.

## 6- مزامنة كلمات المرور (Password synchronization)

تهدف خدمة مزامنة كلمات المرور (password synchronization) لضمان أن المستخدم لديه نفس اسم المستخدم وكلمة المرور في جميع الأنظمة. وبعكس "تسجيل الدخول الأحادي" فإن المستخدم لمزامنة كلمات المرور يقوم بإدخال بيانات المصادقة عند الدخول لكل نظام. ويؤدي تغيير كلمة المرور في نظام واحد إلى نشر هذا التغيير إلى الموارد الأخرى. وهذا يقلل من حرية المستخدم كما قد يقلل الدعم الفني والذى يهدف لإعادة تعيين كلمات المرور.

وعلى عكس "تسجيل الدخول الأحادي" فإن مزامنة كلمات المرور لا تحتوي على مستودع مركزي لكلمات المرور. وبدلاً من ذلك، يقوم كل نظام مزامنة بحفظ نسخة من كلمة مرور المستخدم ويقوم المستخدم مباشرة بالمصادقة على كل نظام. والفائدة التي تعود على المستخدم هي أن هناك كلمة واحدة فقط ليتذكرها. وتستخدم مزامنة كلمات المرور عادة عند دمج عدة أنواع مختلفة من الأنظمة معاً. على سبيل المثال، يجب أن يكون المستخدم قادراً على الوصول إلى تطبيق على شبكة الإنترنت، والوصول إلى تطبيق يعمل على الحاسوب الرئيسي، والوصول أيضاً إلى قاعدة بيانات الحسابات وذلك باستخدام بيانات المصادقة نفسها. وبما أن مزامنة كلمات المرور تحتاج إلى متطلبات قليلة للتنفيذ، فإنها عموماً أقل تكلفة من "تسجيل الدخول الأحادي".

**ومع ذلك فإن مزامنة كلمات المرور لها مشكلاتها الخاصة**. ولأن كلمة المرور نفسها تستخدم في العديد من الموارد فإن اختراق أي من هذه الموارد ُ سيؤدي إلى اختراق جميع الموارد المتزامنة مع المورد المَخترق. وإذا تم استخدام مزامنة كلمات المرور مع موارد ذات متطلبات أمنية مختلفة، فإن المهاجم يستطيع حينها من اختراق الموارد الأقل أمناً للوصول إلى الموارد الأكثر أمناً والتي من المتوقع أن تكون ذات قيمة عالية.

Microsoft

**أمن "مايكروسوفت" في قبضة القراصنة.. كيف ذلك؟ (2023/12/21)**

**في سابقة من نوعها تمكنت مجموعة من القراصنة تسمي نفسها "ستورم-1152" وتنفذ عملياتها من فيتنام من اختراق أمن "مايكروسوفت" وإنشاء ملايين الحسابات المزيفة وبيعها. فكيف يمكن مواجهة مثل عمليات القرصنة هذه؟**

يتم التساؤل الان حول موثوقية أنظمة التحقق المستخدمة عبر **الإنترنت** للتأكد من أنّ مستخدم الشبكة هو إنسان، بعدما كشفت شركة "مايكروسوفت" أخيراً عن مجموعة من القراصنة، في تطوّر يبرز الثغرات في تقنية حروف التحقق المعروفة بـ"كابتشا" والمستخدمة بصورة كبيرة.

فقد كشفت شركة "مايكروسوفت" أن مجموعة قراصنة معلوماتية تسمي نفسها "ستورم-1152" باعت 750 مليون حساب مزيف على خدمات "مايكروسوفت" للسماح للمجرمين على الإنترنت بتنفيذ عملياتهم على الشبكة. وقد استندت في خطواتها إلى التجاوز الآلي لكل ما يجنب الخضوع لشروط المصادقة المطلوبة عند إنشاء حسابات "مايكروسوفت".

هدف **الشبكة** المفضل هي الـ"كابتشا"، وهي نوافذ مستخدمة على نطاق واسع على شبكة الإنترنت، تطلب من المستخدمين إعادة إنتاج سلسلة من الحروف أو الأرقام، أو النقر على أجزاء من صورة تظهر مثلا حافلات أو سلالم، من أجل التأكد من أن المستخدم هو إنسان وليس روبوت. بيد أنّ إجراء المصادقة بدأ بالتقادم، وقد وجد قراصنة "ستورم-1152" طريقة للتحايل عليه، وأتمته، ما أتاح لهم إنشاء ملايين الحسابات المزيفة.

Microsoft

**كيف اخترقوا أمن "مايكروسوفت"؟**

ولتحقيق ذلك، كان هناك بالتأكيد "القليل من التعلم الآلي" وراء ذلك، أي أنّ هؤلاء المتسللين علّموا أداة القرصنة الخاصة بهم كيفية النقر في المكان الصحيح عند عرض صور التحقق، على ما يوضح فرنسوا ديروتي، الخبير في في شركة سيكويا للأمن السيبراني. بعد ذلك، باع قراصنة "ستورم-1152" هذه الحسابات المزيفة على أحد المواقع للأشخاص الذين يريدون تنفيذ هجمات، مثل رسائل البريد الإلكتروني التصيدية أو برامج الفدية أو هجمات الخادم القائمة على حجب الخدمة لجعل الصفحة غير قابلة للوصول، وفق ديروتي. كان اسم المجموعة معروفاً. وفيما تتصدر دول أخرى مثل الصين وروسيا وإيران وكوريا الشمالية عناوين الأخبار في كثير من الأحيان عندما يتعلق الأمر بقرصنة المعلوماتية، فإن فيتنام لديها مجموعات قراصنة تحقق تقدماً في كل عام، على شاكلة الهند أو تركيا، بحسب ديروتي. وقد حجبت "مايكروسوفت" جزءاً من مواقعها على الأراضي الأميركية، وذلك بعد قرار محكمة فدرالية أجازت إغلاق الخوادم التي استضافتها. لكن "من المؤكد أن لديهم مواقع أخرى منتشرة في أماكن أخرى سيتعين إغلاقها من خلال التعاون الدولي، وهو ما يحدث بانتظام"، كما يتوقع الخبير. هناك تقنيات جديدة مثل المصادقة متعددة العوامل، مع الرموز التي يتم تلقيها عبر الرسائل النصية القصيرة على سبيل المثال، لكنها قد لا تستمر لفترة طويلة قبل أن يكتشف المتسللون عيوبها. ومع وجود طرق أخرى مثل مفاتيح الأمان التي توفرها البنوك، يكون الأمان أعلى، لكن نشر هذه الوسائل الجديدة يُعدّ مكلفاً ويستغرق وقتاً طويلاً، في حين لا تزال "مايكروسوفت" تحتفظ بالإصدارات القديمة من برامجها المختلفة.