Hash password algorithm (recommend)

Argon

PBKDF2

Bcrypt

(Basic) SHA-2

SHA-1

SHA-3

Lecture 3: User Authentication Ep.2

MD5 = 2^{128} ตัว

05506044 System Security

Dr. Rungrat Wiangsripanawan

powershell

→ func generate hash

Secure Hash algorithm = SHA1

↳ output 160 bit

SHA2 → 256, 384

SHA2-512

Last Modified: 19.08.65

Objective 1.

Understand and being able to explain

- Four basic ways to help users with the memorable passwords I
- Master Passwords
- Token-based User Authentication
  - Memory Cards
  - Smart Cards
- Biometric Authentication

Explain = Know meaning and can give Examples

Objective 2.

Understand and being able to explain

- Two factor Authentication / Multifactor Authentication
- Two Step verification
- CAPTHA

Explain = Know meaning and can give Examples

Four basic ways to help users with the memorable passwords I

User Education

- **provides users** with the **guidelines** on password selection
  - Ex. Use the first letter of the phrase
  - **NIST** Password Guidelines

Computer Generated Password

- FIPS PUB 181 one of the best **designed automated password**
  - Find pronounceable syllables, concatenating them to form a word
- **Drawback**
  - If the passwords are quite random, **users can't remember**

Reactive password checking

Proactive password checking

Reactive Password System

- ระบบจะรันโปรแกรม password cracker เองเลยเป็นช่วงๆ (periodically runs its own password cracker)
  - ถ้าเจอว่า pwd ใคร โปรแกรมนี้เดาได้ จะยกเลิกพาสเวิร์ดนี้
  - และแจ้งผู้ใช้
- ตัวอย่างโปรแกรม pwd cracker Jack the Ripper password cracker (openwall.com/john/pro)
- Drawbacks (ข้อเสีย)
  - Resource intensive ใช้รีซอร์สมาก
  - Until the password checker finds them, the guessable passwords remain effective.

Proactive password checker

- อนุญาตให้ผู้ใช้เลือก pwd ของตัวเอง
  - แต่เมื่อผู้ใช้ตั้ง pwd เองแล้ว
  - ระบบจะเช็ค ณ เวลานั้นเลยว่า pwd นี้ระบบจะอนุญาตให้ใช้หรือไม่
  - ถ้าไม่ จะไม่อนุญาตให้ใช้พาสเวิร์ดนี้ ผู้ใช้ต้องสร้างใหม่ (จนกว่า พาสเวิร์ดของผู้ใช้ เป็นไปตามกฎพาสเวิร์ดที่ดี หรือไม่ได้โดนแครกได้ง่ายจากโปรแกรมแครกเกอร์ที่ระบบมี ระบบจึงจะอนุญาตให้ใช้พาสเวิร์ดนั้น)
- with adequate guidance from the system, users can select memorable passwords from a very large space that are not likely to be guessed in a dictionary attack.

Proactive password checker: **Possible approaches**

- **Rule Enforcement**
- **Password Cracker.**
- **Markov Model**
- **Bloom Filter**

Proactive password checker: II

Rule Enforcement

- 8 ตัวอักษร
- มีทั้ง uppercase, lowercase และ digits and etc.

Password Cracker.

- Run a large dictionary of possible bad password
- Problems.
  - Space: the dictionary must be very large to be effective
  - Large dictionary – large time.

***http://www.openwall.com/articles/PHP-Users-Passwords#enforcing-password-policy *** สำหรับ PHP

Proactive password checker: II

Markov Model

- generates guessable passwords โดยใช้โมเดลนี้
- ถ้า พาสเวิร์ดไหนถูก gen จากโมเดลนี้ได้ ไม่ให้ใช้

Bloom Filter

- เป็นวิธีการหนึ่งในการสร้าง table ของ hash จากคำใน dictionary เพื่อให้ค้นหา พาสเวิร์ดที่ตรงกับคำใน dict ได้เร็วขึ้น

Rainbow Table

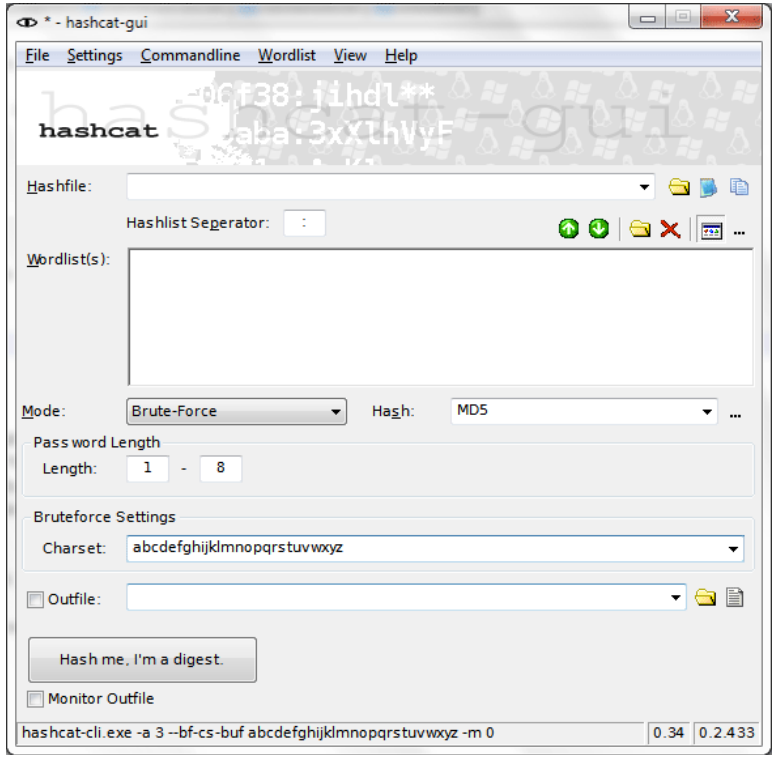
Note....

- ในปัจจุบัน ซอฟต์แวร์ password cracker สามารถ brute force crack ได้ถึง 8 ตัว
- นอกจากซอฟต แวร์แล้วสามารถแครกพาสเวิร์ดเร็วกว่า ถูกกว่าใช้ไฟน้อยกว่าโดยใช้ hardware เช่น GPU or FPGAs.
- การ crack password ยาวกว่า 8 ตัวอักษร ต้องใช้ FPGA-based device (ฮาร์ดแวร์)

http://2.bp.blogspot.com/-IEWl9KCMnQ0/TgJTJVdstRI/AAAAAAAAAXc/cGOR1nTYegs/s1600/bitcoin-mining-rig1.jpg

Hashcat [wiki]

- the self-proclaimed world's fastest CPU-based password recovery tool.
- Just released as free software in 2015
- Versions are available for Linux, OSX, and Windows
- hashcat come in CPU-based - GPU-based variants.
- clHashcat/cudaHashcat - A GPU-accelerated tool (OpenCL or CUDA)



http://www.question-defense.com/wp-content/uploads/2010/08/hashcat-gui-with-basic-brute-force-settings-and-lowercase-charset.gif

Password cracking using GPU

MD-5

- **PBKDF2 SHA-256**. *Password table for cracking a PBKDF2 hash function using an RTX 3090 GPU.*

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	2 secs	4 secs	4 secs
5	Instantly	3 secs	2 mins	4 mins	12 mins
6	Instantly	1 min	1 hour	4 hours	15 hours
7	3 secs	35 mins	3 days	2 weeks	2 months
8	26 secs	15 hours	5 months	2 years	10 years
9	4 mins	2 weeks	23 years	100 years	800 years
10	44 mins	1 year	1k years	7k years	61k years
11	7 hours	31 years	63k years	435k years	5m years
12	3 days	800 years	3m years	27m years	363m years
13	1 month	21k years	170m years	2bn years	28bn years
14	10 months	539k years	9bn years	104bn years	2tn years
15	8 years	14m years	460bn years	6tn years	166tn years
16	84 years	365m years	24tn years	399 tn years	13 qdn years
17	800 years	9bn years	1qdn years	25 qdn years	983 qdn years
18	8k years	246bn years	65 qdn years	2 qntn yrs	76qntn years

https://www.hivesystems.io/blog/are-your-passwords-in-the-green

If your password is secured?
Example of Password Checker tools

- NordPass Password Strength Checker
  - https://nordpass.com/secure-password/

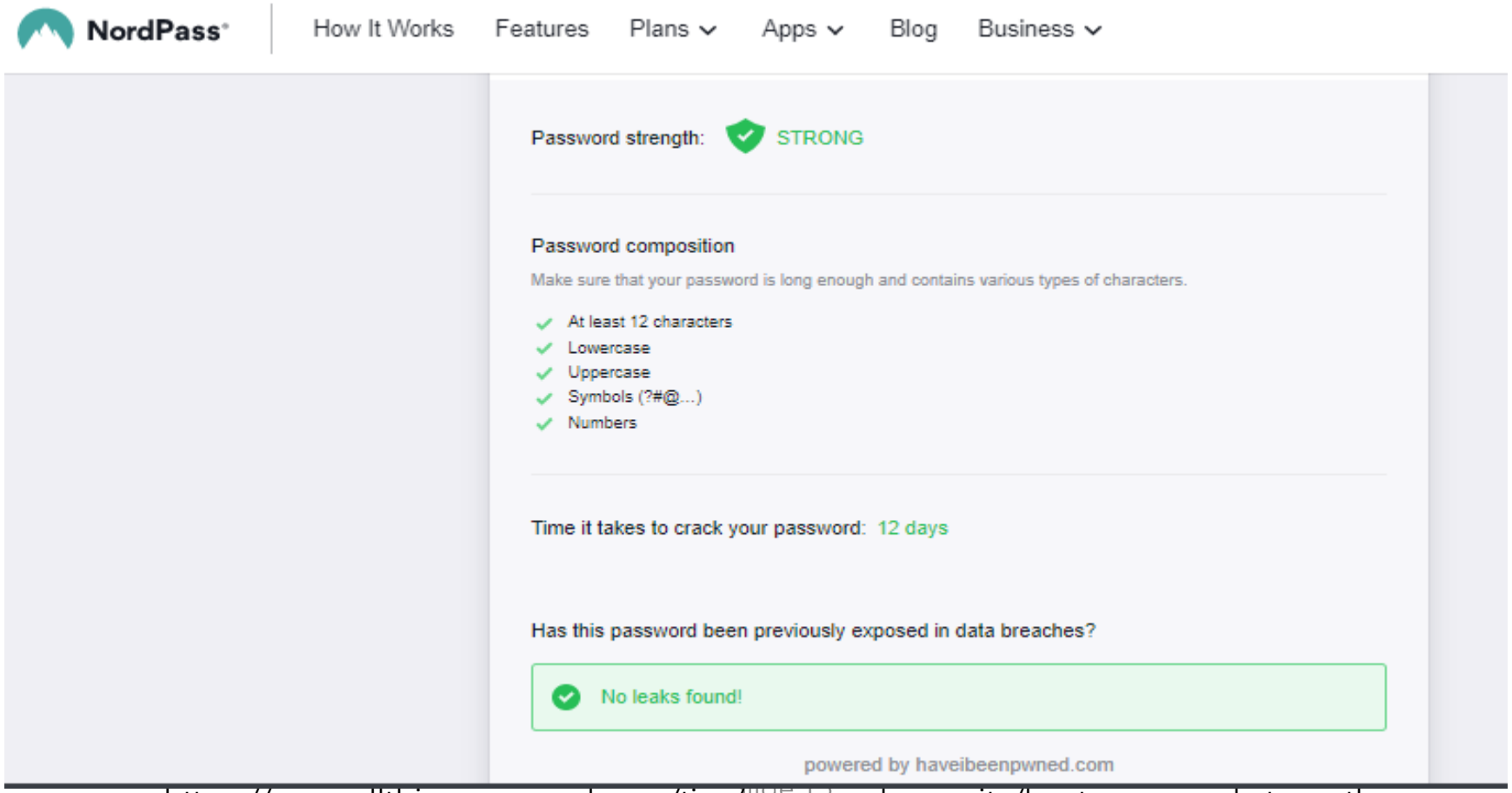
- All Things Secured Password Strength Checker
  - https://www.allthingssecured.com/password-checker/

- Kaspersky Password Strength Meter
  - https://password.kaspersky.com/

Be careful don't use your password to try .. Use others password type characters that are similar to your password, but don't type in your actual password

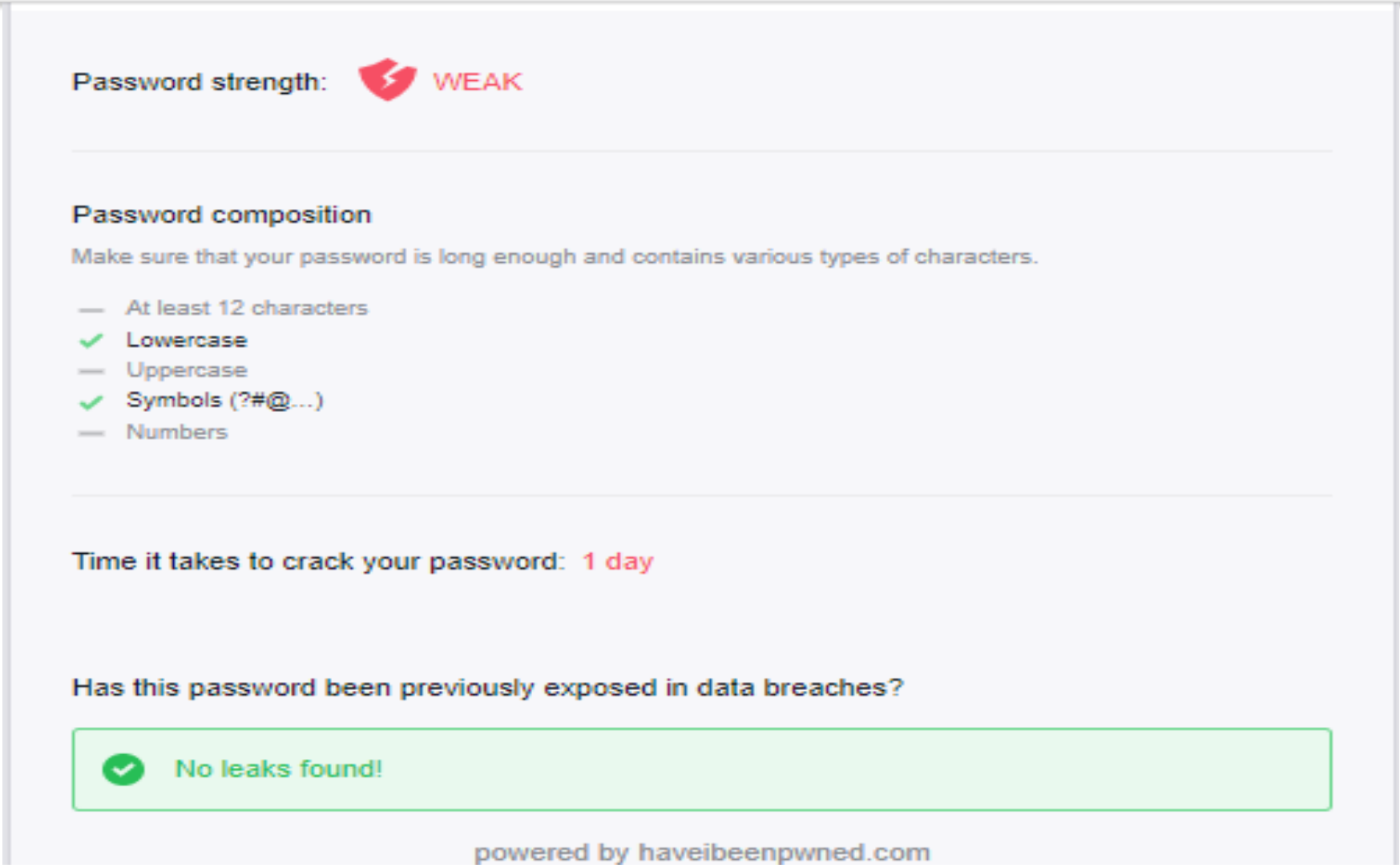
Example of Password Checker tools

- NordPass Password Strength Checker : Strong pwd



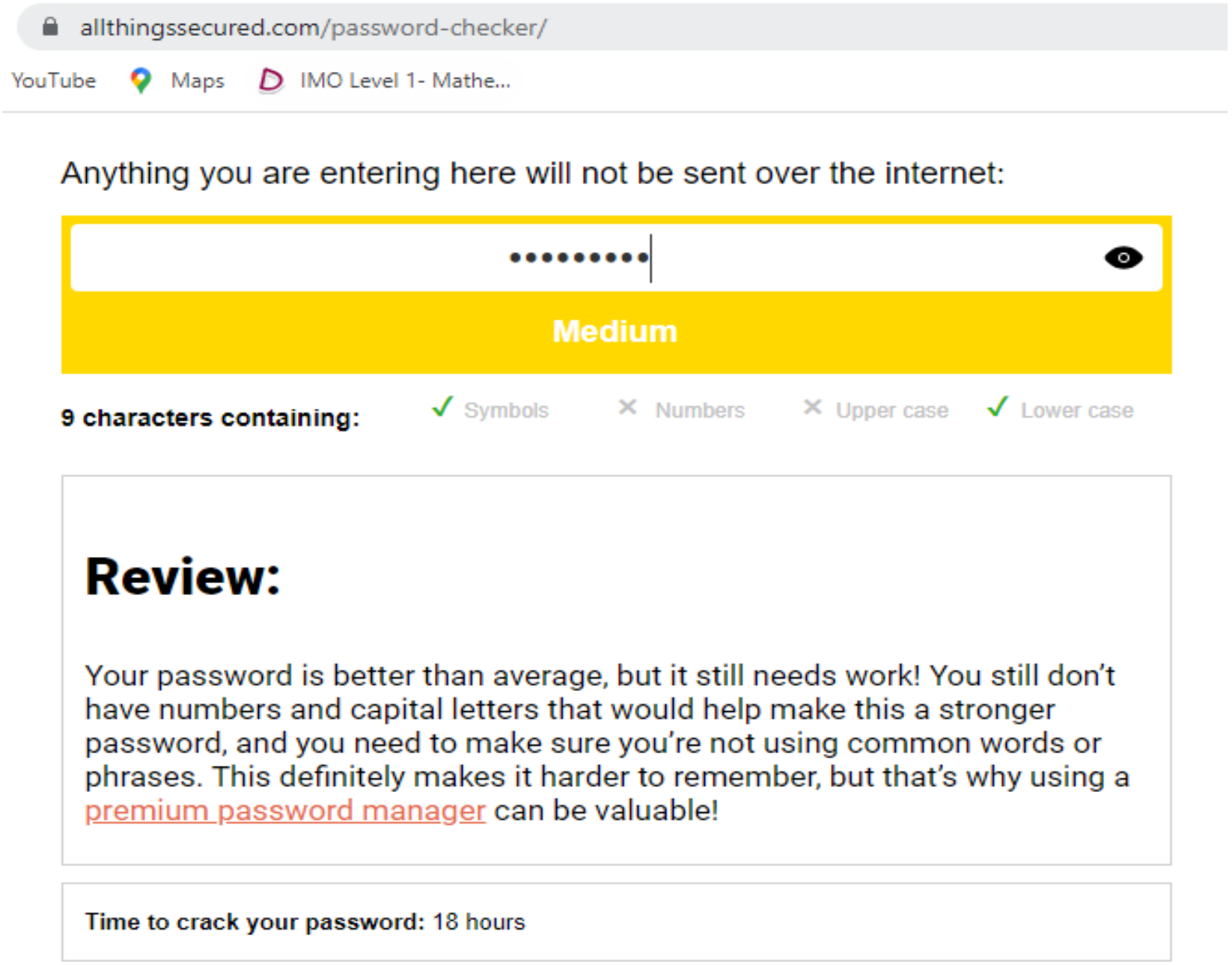
https://www.allthingssecured.com/tips/password-security/best-password-strength-checkers/#nordpass

NordPass Password Strength Checker : Weak pwd

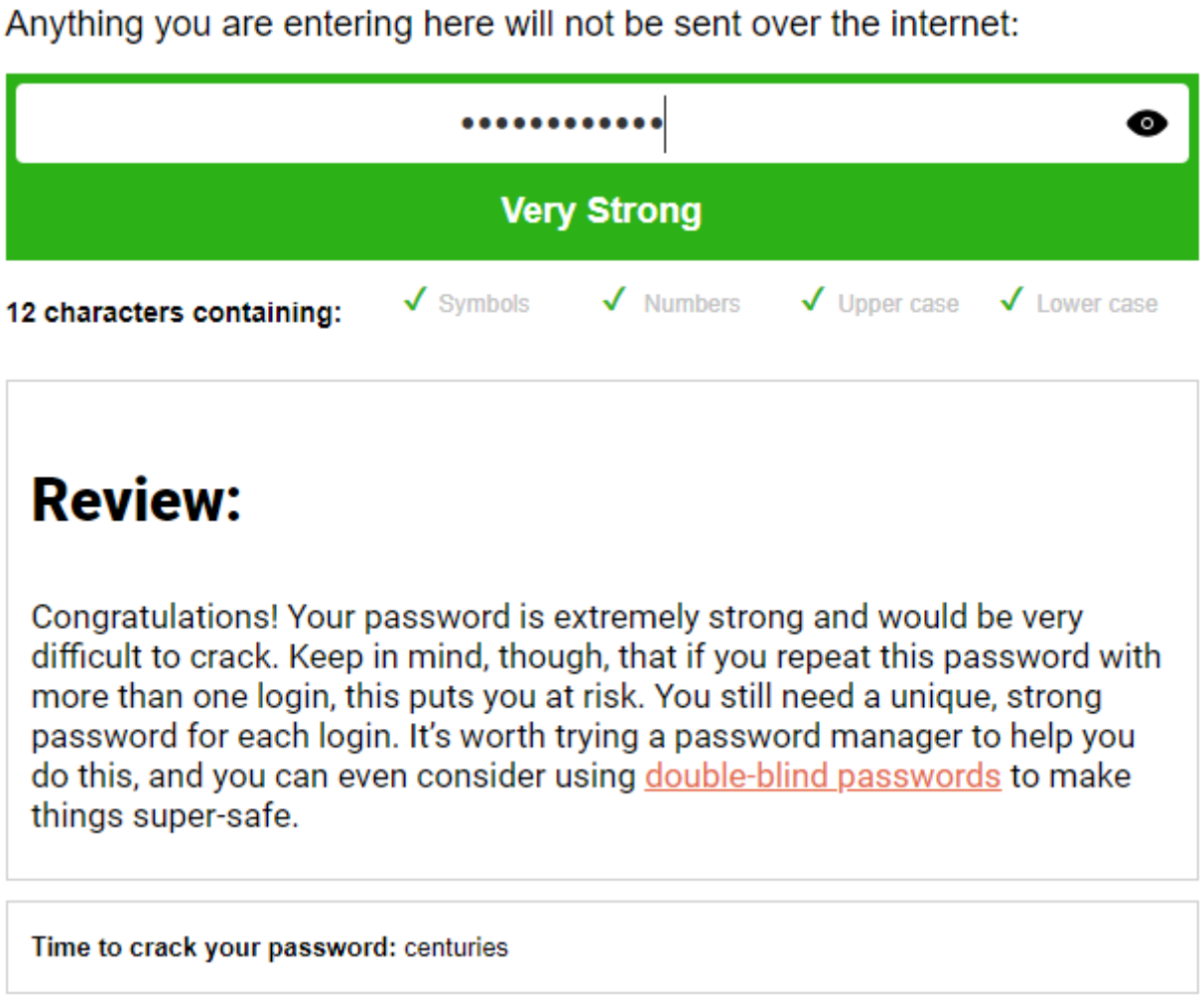


All Things Secure Password Checker : weak pwd

https://www.allthingssecured.com/tips/password-security/best-password-strength-checkers/#allthingssecured

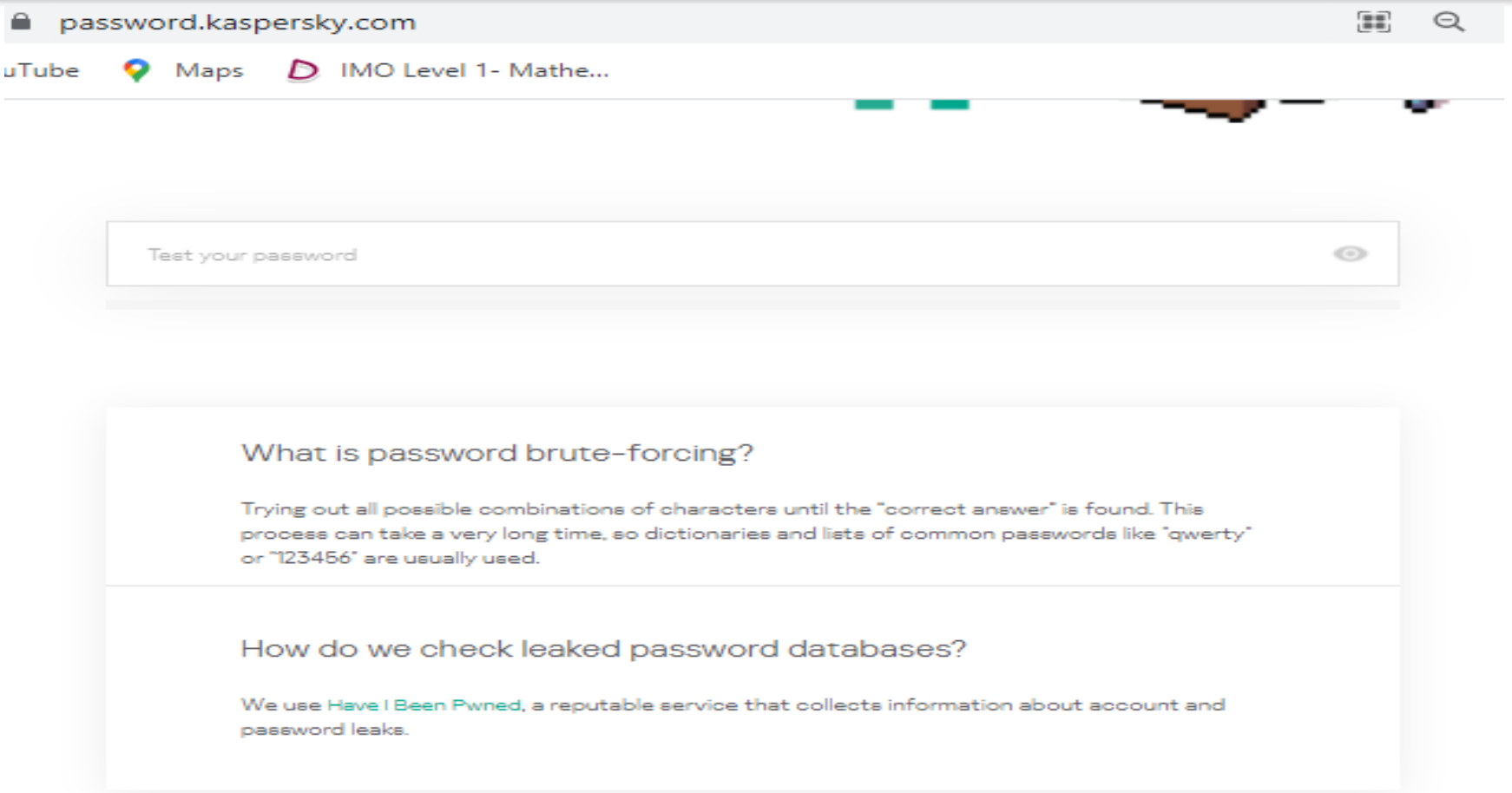


All Things Secure Password Checker : Strong pwd



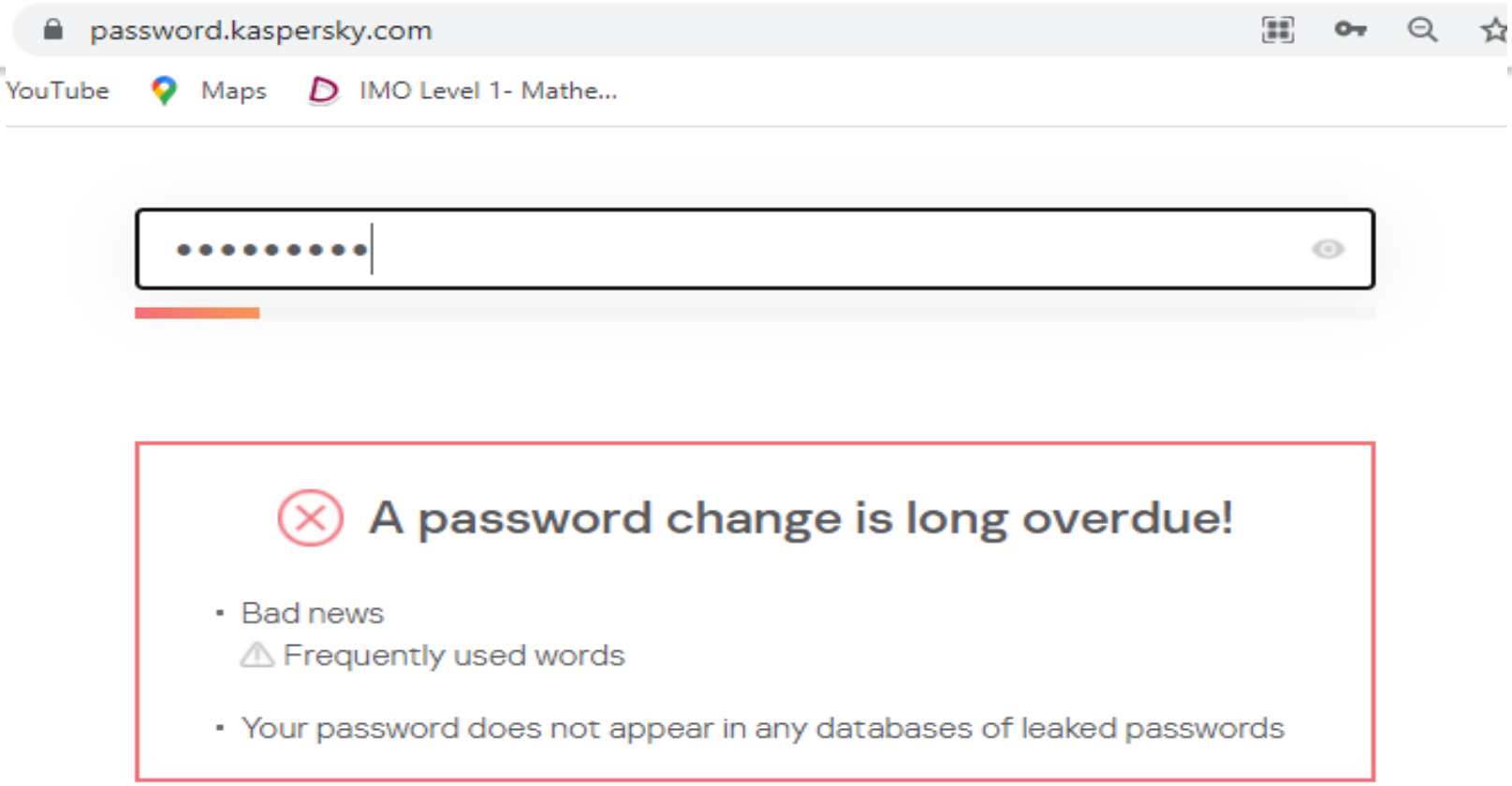
https://www.allthingssecured.com/tips/password-security/best-password-strength-checkers/#allthingssecured

Kaspersky Password Strength Meter



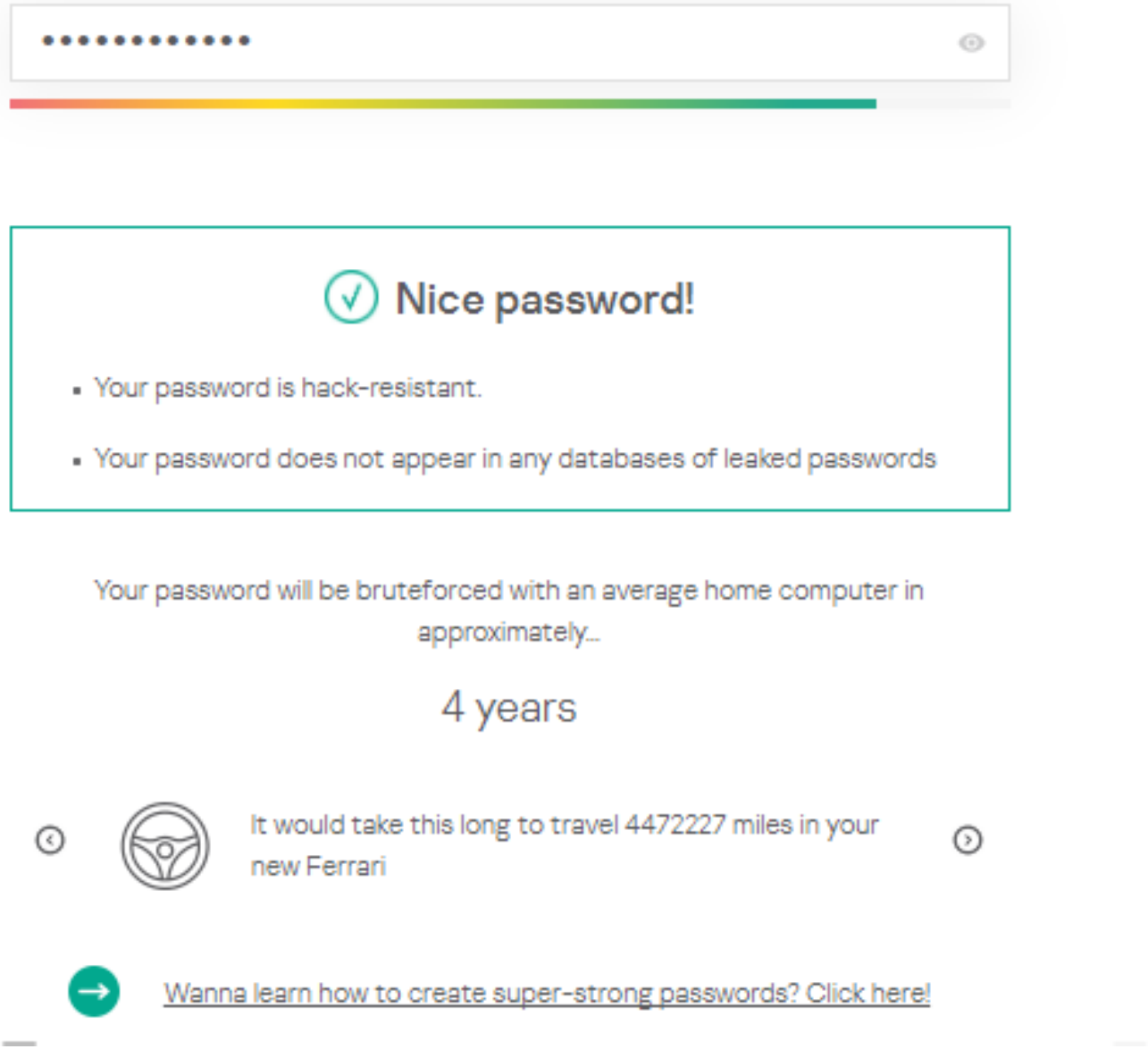
https://password.kaspersky.com/

Kaspersky Password Strength Meter : Weak Pwd



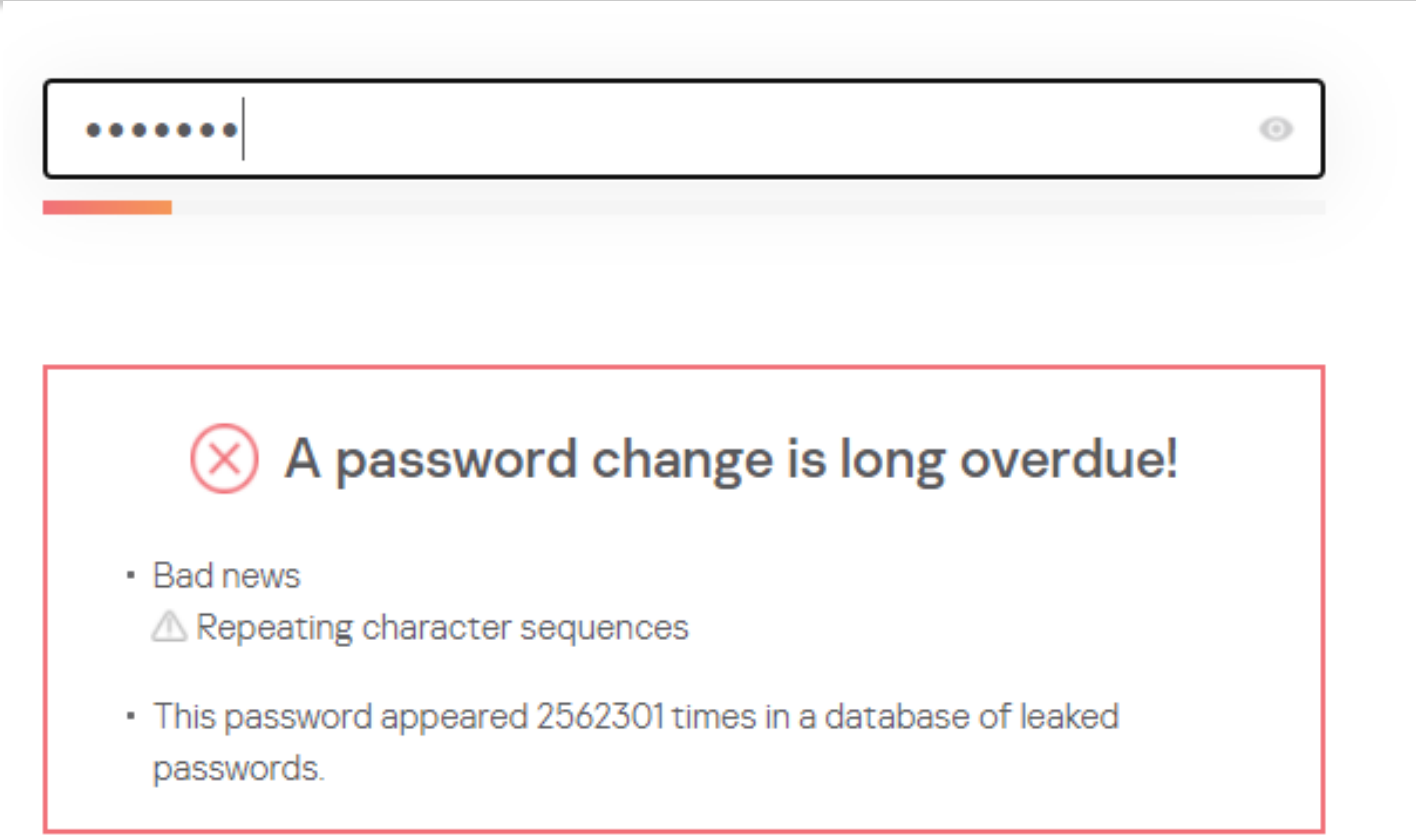
https://password.kaspersky.com/

Kaspersky Password Strength Meter : Strong Pwd



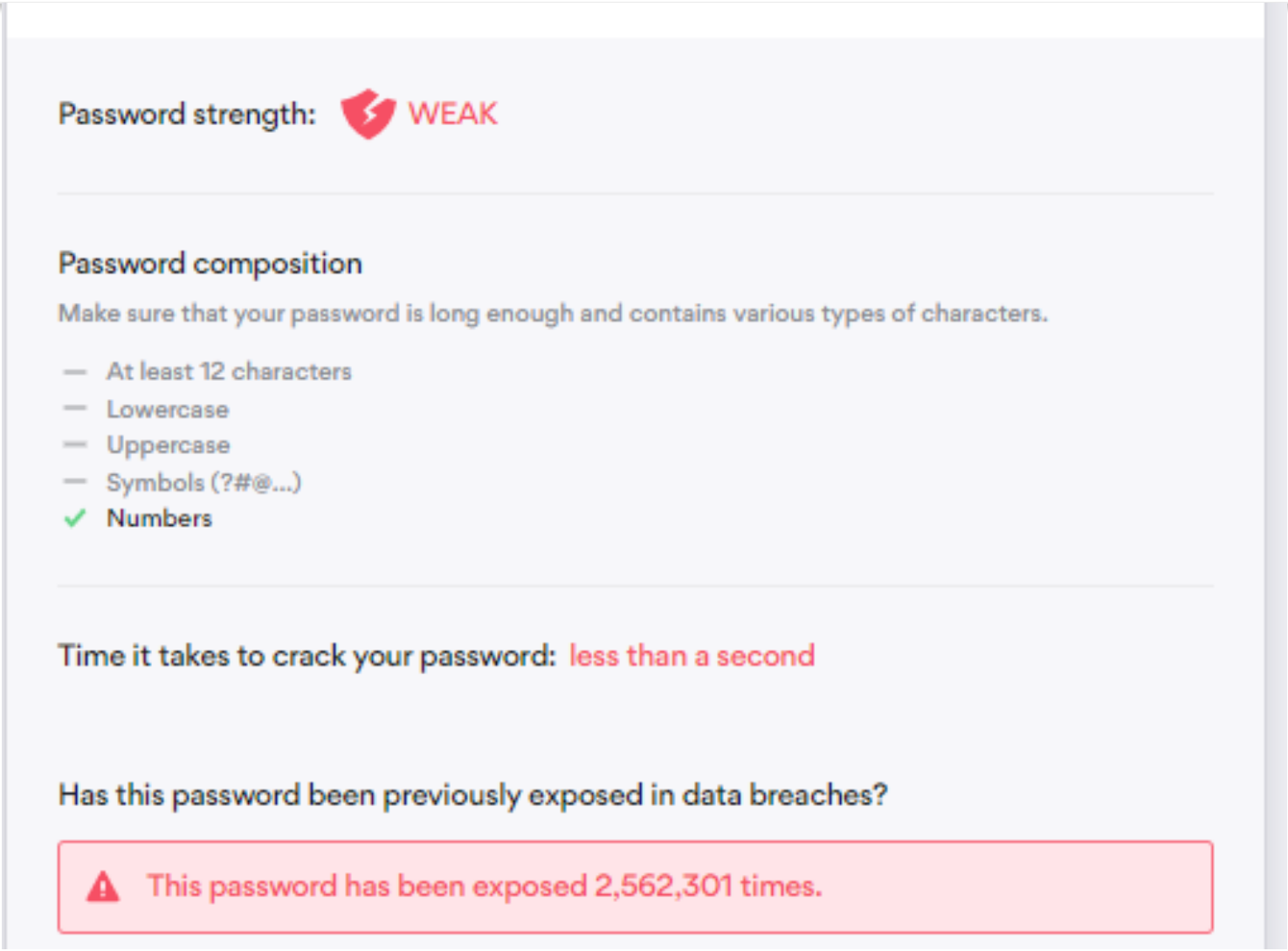
https://password.kaspersky.com/

Kaspersky Password Strength Meter :1234567



https://password.kaspersky.com/

NordPass Password Strength Checker : 1234567



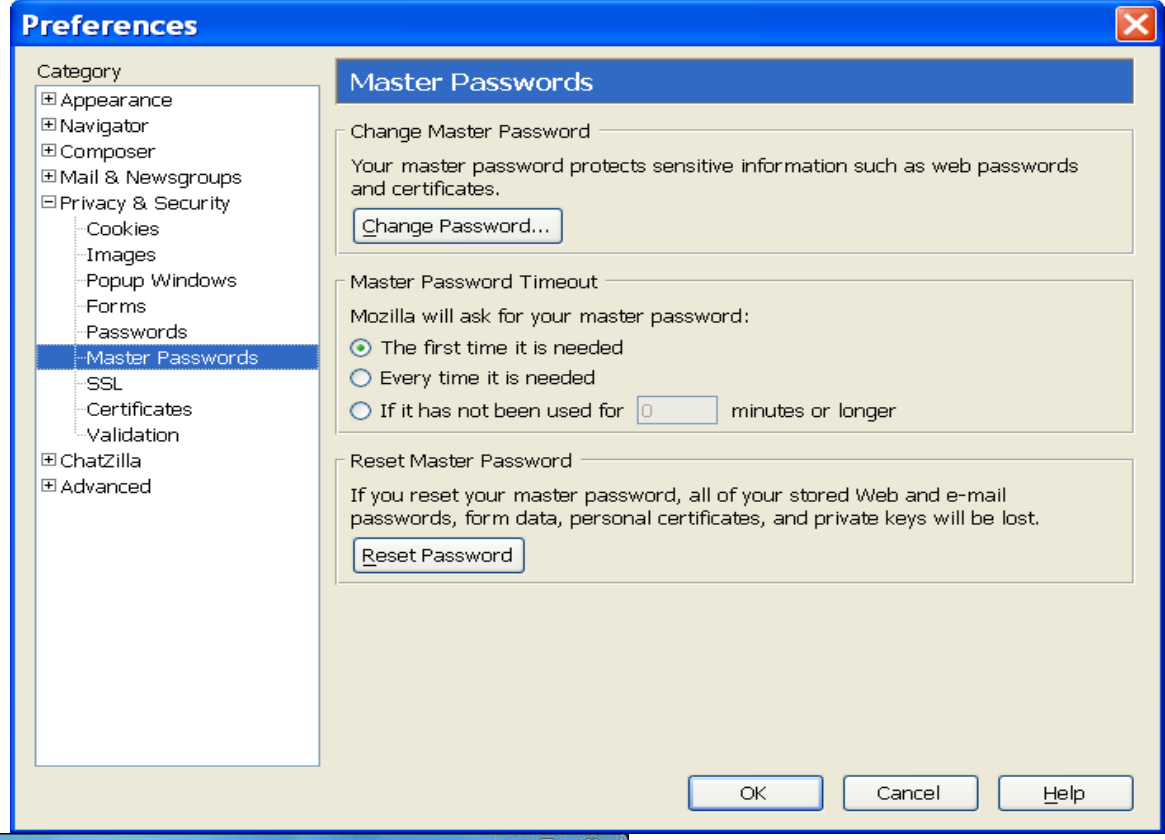
Master passwords or password masters

- แทนที่จะจำพาสเวิร์ดมากมาย ซึ่งส่วนใหญ่อาจเป็นพาสเวิร์ดที่เดาง่าย ใช้ซ้ำ กรณีนี้จำพาสเวิร์ดเดียวคือ master password.
- The idea is you make the master password a good one, apply the appropriate rules like changing every so often, and never remember any of the others at all.
- **Don't forget this one though!**
- ปัจจุบัน feature ของ master password จะมากับโปรแกรมประเภท Password manager

Examples

Software based.

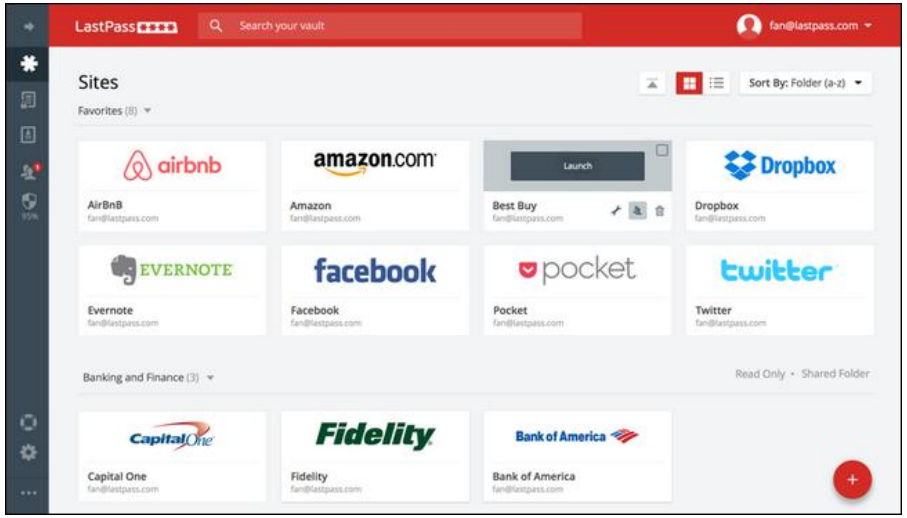
- Master password in Firefox privacy option

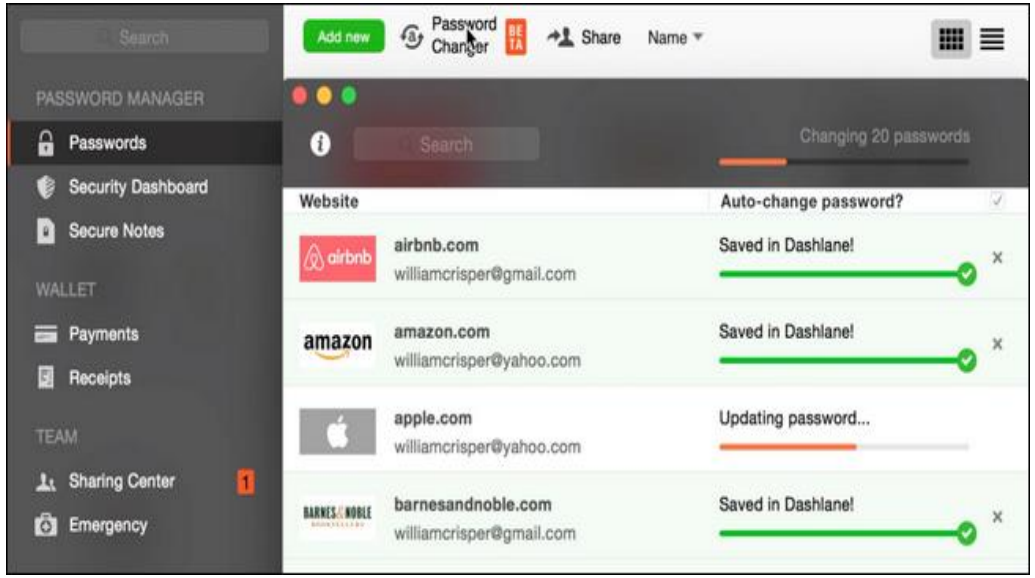


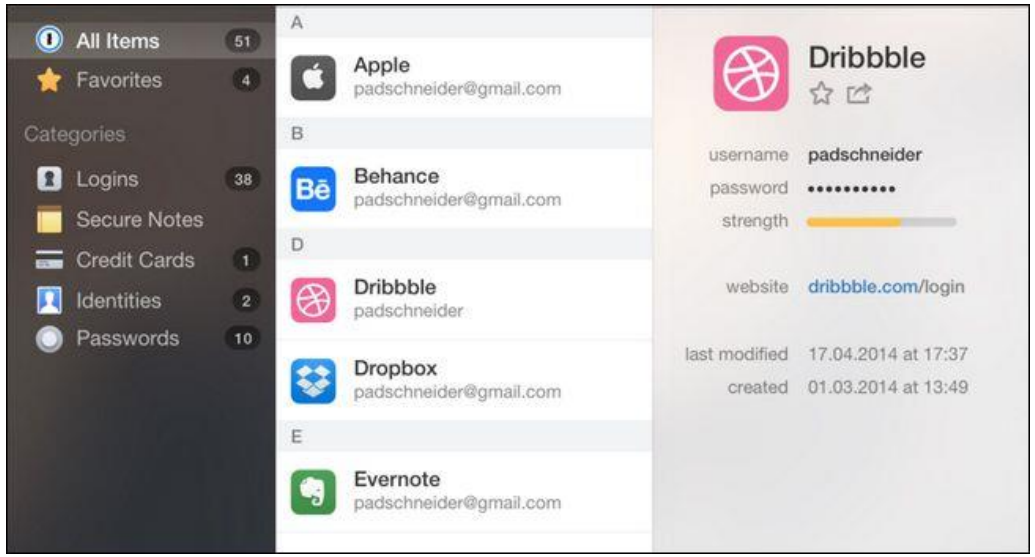
Password manager

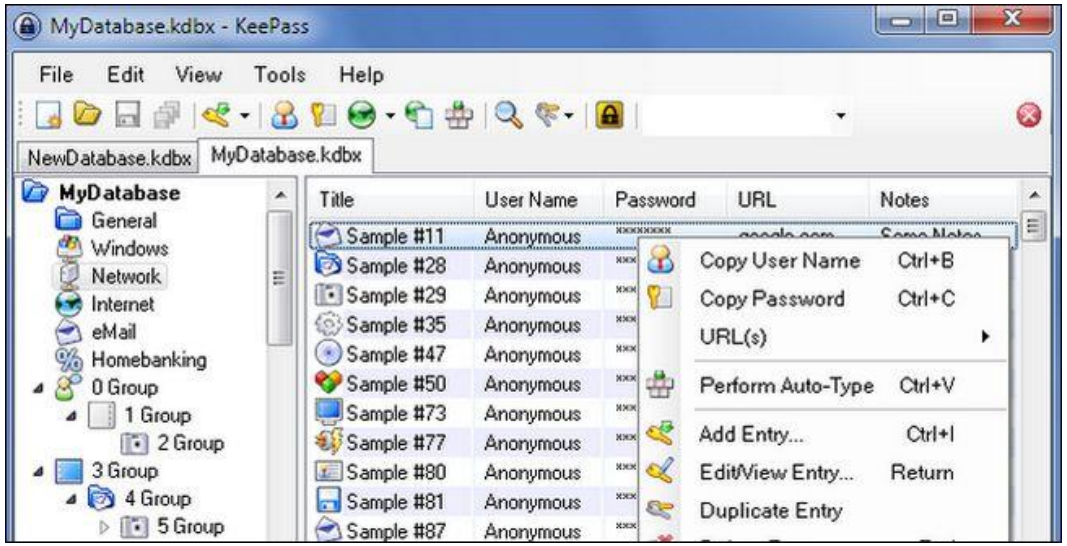
- ซอฟต์แวร์หรือแอพพลิเคชันที่ช่วยในการบันทึก บริหาร และ จัดการรหัสผ่าน
- หลังจากผู้ใช้ทำการบันทึกรหัสผ่านของ site ต่างๆ หรือ เครื่องต่างๆ ที่ต้องการเข้าถึง โปรแกรมจะจัดการเก็บรหัสผ่านให้ ผู้ใช้เพียงจำ Master password เพื่อเข้าถึงโปรแกรมให้ได้
- โปรแกรมนี้ต้อง มีการเก็บรหัสผ่านอย่างปลอดภัย รหัสผ่านอาจจะถูกเก็บที่เครื่องของผู้ใช้ หรือ บนคลาวด์ หรือ ทั้งสองที่
- นอกจาก feature master password จะมี feature อื่นๆ เช่น มีตัวช่วยในการสร้างรหัสผ่าน ตัวกรอกรหัสผ่าน อัตโนมัติ ฯลฯ
- Examples of Password Manager
  - Lastpass Dashlane Keepass 1Password RoboForm

- Lastpass Dashlane Keepass 1Password RoboForm





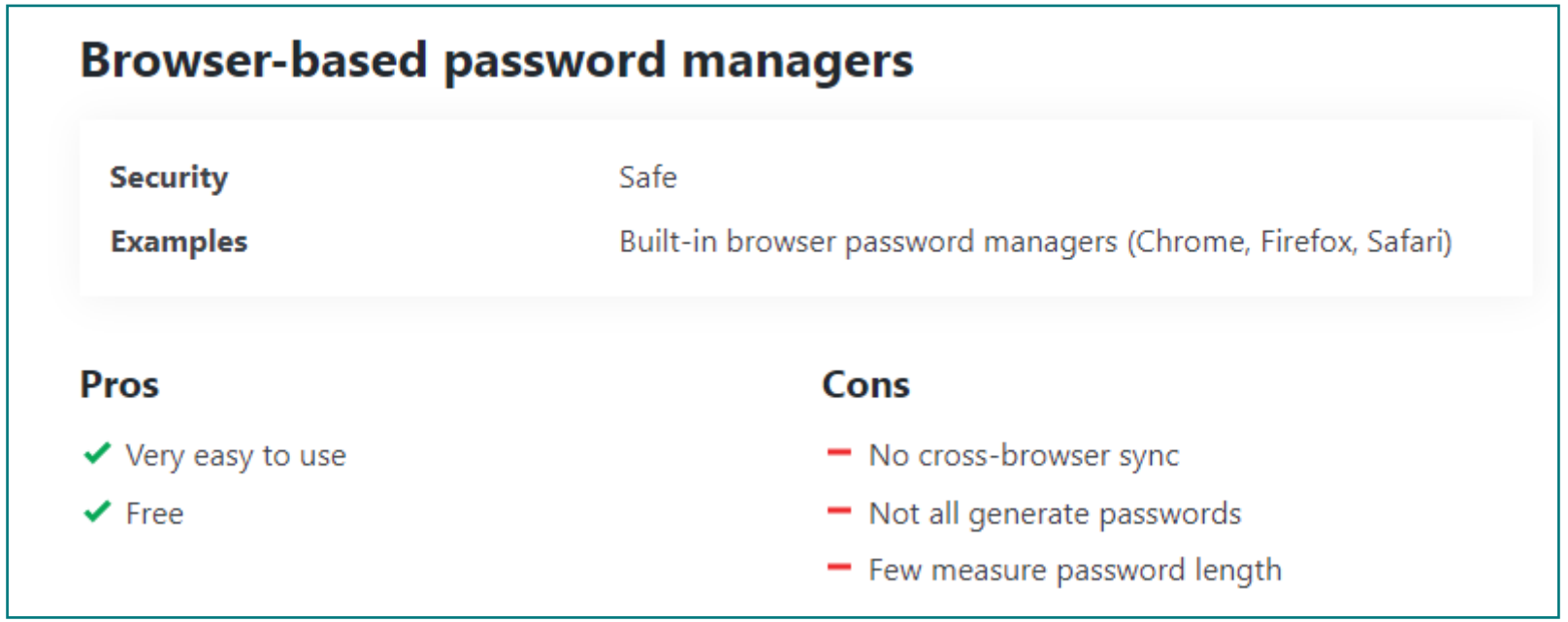




http://www.howtogeek.com/240255/password-managers-compared-lastpass-vs-keepass-vs-dashlane-vs-1password/

รูปแบบ Password Manager
Browser based:

- **https://cybernews.com/best-password-managers/are-password-managers-safe/**



Browser-based password managers

Security	Safe
Examples	Built-in browser password managers (Chrome, Firefox, Safari)

Pros

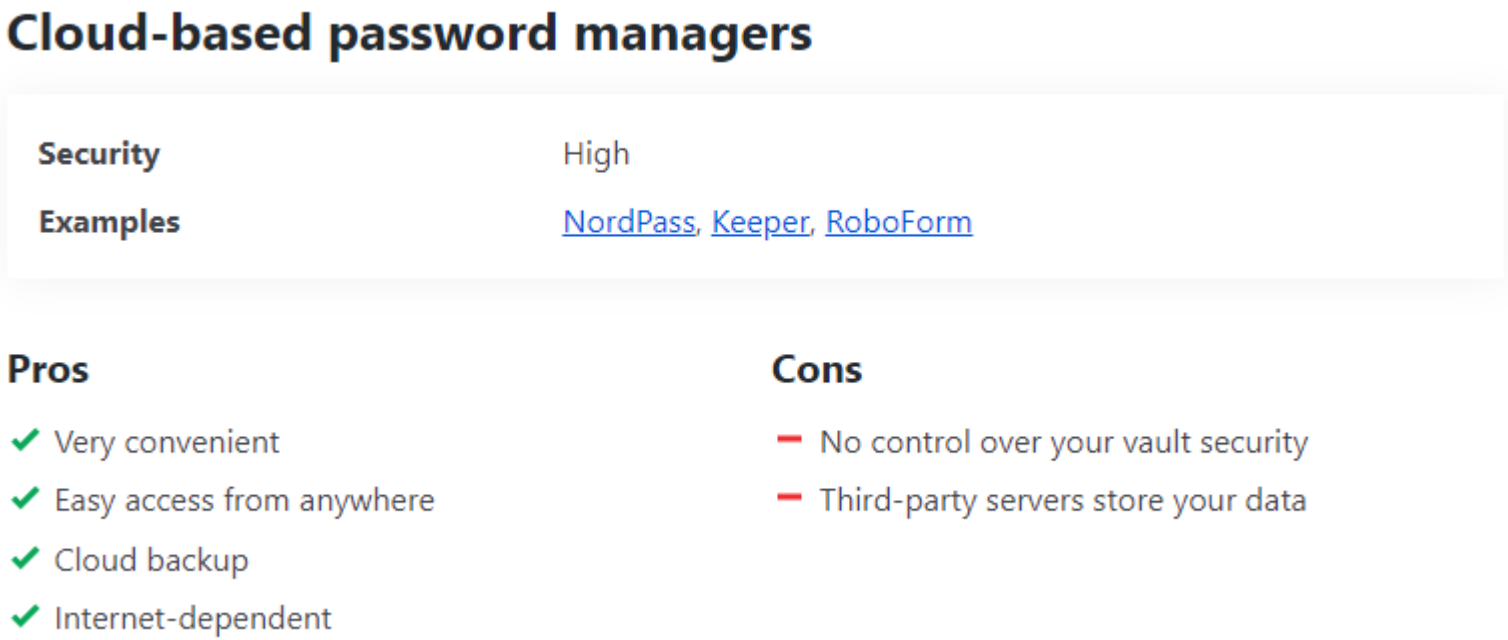
- ✔ Very easy to use
- ✔ Free

Cons

- ━ No cross-browser sync
- ━ Not all generate passwords
- ━ Few measure password length

รูปแบบ Password Manager
Cloud-based

- **https://cybernews.com/best-password-managers/are-password-managers-safe/**



Cloud-based password managers

Security	High
Examples	NordPass, Keeper, RoboForm

Pros

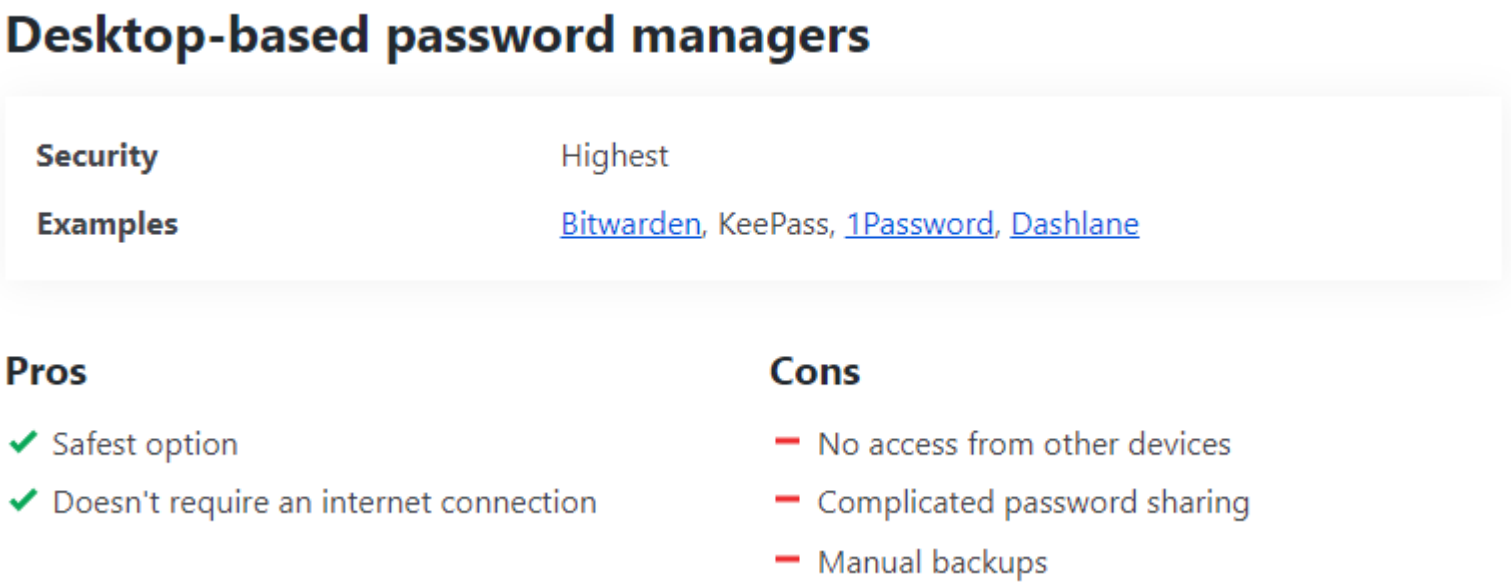
- ✔ Very convenient
- ✔ Easy access from anywhere
- ✔ Cloud backup
- ✔ Internet-dependent

Cons

- ━ No control over your vault security
- ━ Third-party servers store your data

รูปแบบ Password Manager
Desktop-based

- **https://cybernews.com/best-password-managers/are-password-managers-safe/**



Desktop-based password managers

Security	Highest
Examples	Bitwarden, KeePass, 1Password, Dashlane

Pros

- ✔ Safest option
- ✔ Doesn't require an internet connection

Cons

- ━ No access from other devices
- ━ Complicated password sharing
- ━ Manual backups

นักศึกษาคิดว่า ปัญหาของ Password Manager คืออะไร

- **Are password managers safe to use in 2022?**
  - **https://cybernews.com/best-password-managers/are-password-managers-safe/**

Password Manager Breaches/Crack I

- **2014**
- **LastPass, My1Login, NeedMyPassword, PasswordBox, and RoboForm**: Researchers at the University of California Berkeley discovered a number of vulnerabilities in a handful of password managers. “In four out of the five password managers they studied, an attacker can learn
  - a **user's credentials for arbitrary websites**,” researchers Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song wrote in their paper.
- **RoboForm**: IT security consultant and tech enthusiast Paul Moore discovered one critical vulnerability in and a privacy loophole in the password management service that could allow attackers and prying eyes to obtain users' personal data,
  - including **stored login credentials** of various websites and even **card payment detail**

สุดแล้ว

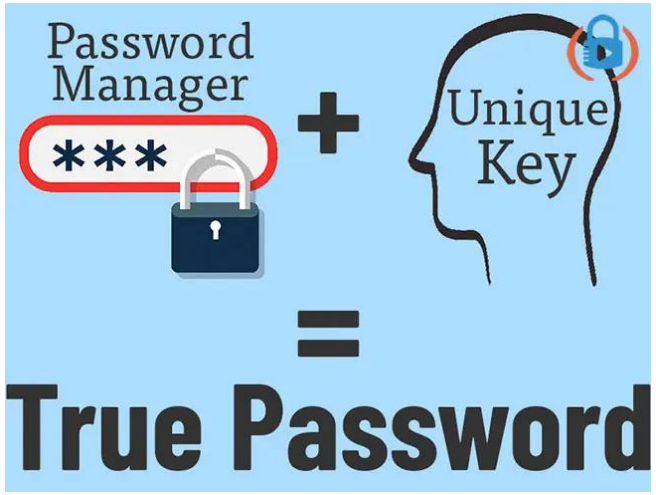
Password Manager Breaches/Crack II

- **2015**
- **KeePass**: When KeeFarce (a hacking tool) program runs on a computer where a logged in user has the KeePass database unlocked,
  - it **decrypts the entire database** and writes it to a file that the hacker can easily access.
  - In theory this kind of hack makes all password managers vulnerable.
- **LastPass**: An intrusion to the company's servers was detected. While encrypted user data wasn't stolen, cyber criminals **stole**
  - account email addresses, password reminders, server per-user salts, and authentication hashes.

Double Blind Password

ส่วนที่ 1 store ไว้บนเครื่อง
ส่วนที่ 2 user จำ

ถ้าจะ hack ต้อง brute force ตรงนี้



https://www.allthingssecured.com/wp-content/uploads/secure-password-equation.jpg.webp

Password Summary:

- การใช้ password ในการ authen มีปัญหามากมาย
- โดยเฉพาะอย่างยิ่งการที่จะต้องตั้งพาสเวิร์ดและหาวิธีจำอย่างปลอดภัย และเปลี่ยนพาสเวิร์ด ตามระยะเวลาที่กำหนด ทำให้การตั้งพาสเวิร์ดที่ดี (จำไม่ยาก) เป็นเรื่องที่ยาก
  - ยิ่งไปกว่านั้น เช่น ในกรณี ของเว็บไซต์ ถ้าเว็บไซต์ที่เราต้องเข้า access จำนวนมากนั้น ต้องใช้ passsword ในการ พิสูจน์ตัวตน ปัญหาเรื่องการตั้งจำ และ เปลี่ยน พาสเวิร์ด ก็จะมากขึ้นไปอีก หลายเท่าตัว
  - การใช้พาสเวิร์ดเดียวกัน ในการ เข้าถึง เว็บไซต์ต่างกัน => bad idea มาก
  - ยิ่งไปกว่านั้น พาสเวิร์ด
  - พาสเวิร์ดจะ ถูกโจมตีได้ง่าย (vulnerable) ต่อ การ attack แบบ social engineering**, หรือ communication eavesdropping

โจมตีผ่านพฤติกรรม user

- พาสเวิร์ด เป็น การ Authen แบบ something the user knows
- ยังมีวิธีการ authen แบบอื่นๆ อีก
  - We will first look at using passwords but in such a way as to alleviate the memory problem

***การโจมตีโดยไม่ได้ใช้วิธีการทาง Technical แต่ใช้ช่องโหว่จากพฤติกรรมของผู้ใช้

Factor ที่สอง - สิ่งที่มี

How about something the user has/posses/holds

physical - hard tokens

- in other words 'Token-based Authentication'
- Tokens – objects that a user posses.
- The user has to present a physical token to be authenticated.
- Examples: keys, cards or identity tags (access to buildings) [5]
- We will examine the two types of token widely used.

Memory cards	**Smart cards**

Memory Cards: store but do not process data

The common one is the bank card with a magnetic stripe on the bank.

A magnetic stripe can store

- **a simple security code**
- **and some information**

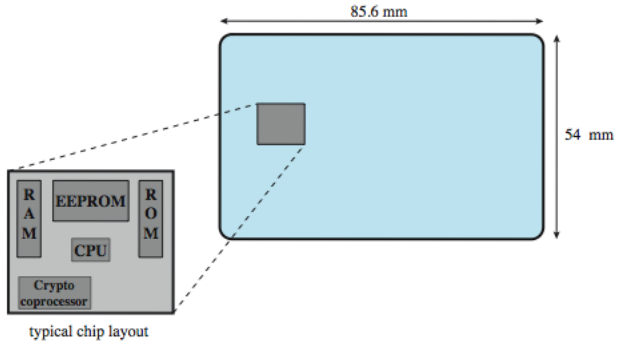
This can be read by an inexpensive(programmable) card reader.

Can be used alone for physical access such as a hotel room.

For *authentication*, used with some forms of password or PIN (personal identification number)

Smart Cards

- Most important category of smart token is the smart card
  - Credit-card appearance, has an electronic interface and can use any type of authentication protocols.



typical chip layout

- What are inside the smart card's chip?

Processor	Memory	I/O ports	Crypto co-processor (optional)

Smart Tokens **three dimensions =>**

Physical characteristics

ฝังตัว

- The smart token will include an embedded microprocessor.
- A smart card - the token that looks like a bank card.
- Or, they can look like calculators, keys or other small portable objects.

Interface

อย่างใดอย่างหนึ่ง

- Manual interface: a keypad and display for human/token interaction
- Electronic interface: communicate with a compatible reader/writer

Authentication protocol:

Token based: Some drawbacks

สิ่งที่ต่างกัน เวลาแปะคีย์การ์ด

Require special readers	• Increases cost and creates the requirement to maintain the security of the reader's HW and SW
เป็นเจ้าของบัตรจริงไหม Token loss	• Prevent its owner to gain access to the system เจ้าของใช้ไม่ได้
Token stolen	• Anybody who is in possession of the token has the same rights as the legitimate owner. คนขโมยเอาไปใช้ได้
User dissatisfaction	• It's okay to use for ATM but not computer.

USB dongle

- A house-key size flash memory device plugged into the USB port to verify a user's identity
- Has the same functionality as the smart card.
- Used by
  - Individual laptop user access the company network
  - Software makers seeking to prevent private use of their product.
- Advantage over smart card
  - Doesn't need a card reader.

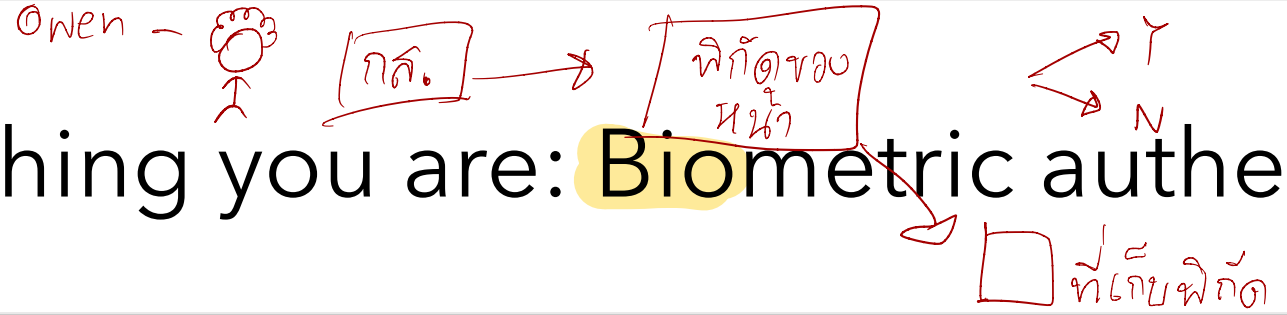
Remark:

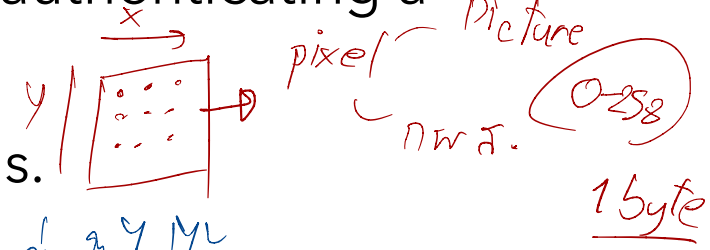
- To increase security, physical tokens are often used in combination with something you know, e.g. bank cards come with a PIN or with a photo of the user.
- (เพื่อความปลอดภัย ปกติใช้ร่วมกับ factor อื่น)

Next=> Something you are

Something you are: Biometric authentication

- Authenticated based on the user's unique physical characteristics.
  - (traits, features) of a person such as face, finger prints, iris patterns, hand geometry (maybe even DNA at some time in the future). [5]
- Biometrics may seem to offer the most secure solution for authenticating a person.
- Complex and expensive compare to passwords and tokens.
- Based on
  - pattern recognition
  - Hence, accuracy concept is involved (how closely it is matched)
  - accuracy doesn't apply with passwords and tokens หมายความว่า ???





False Negative – เป็น owen แต่เข้าไม่ได้
False Positive – เป็น owen เข้าถึงได้น้อย

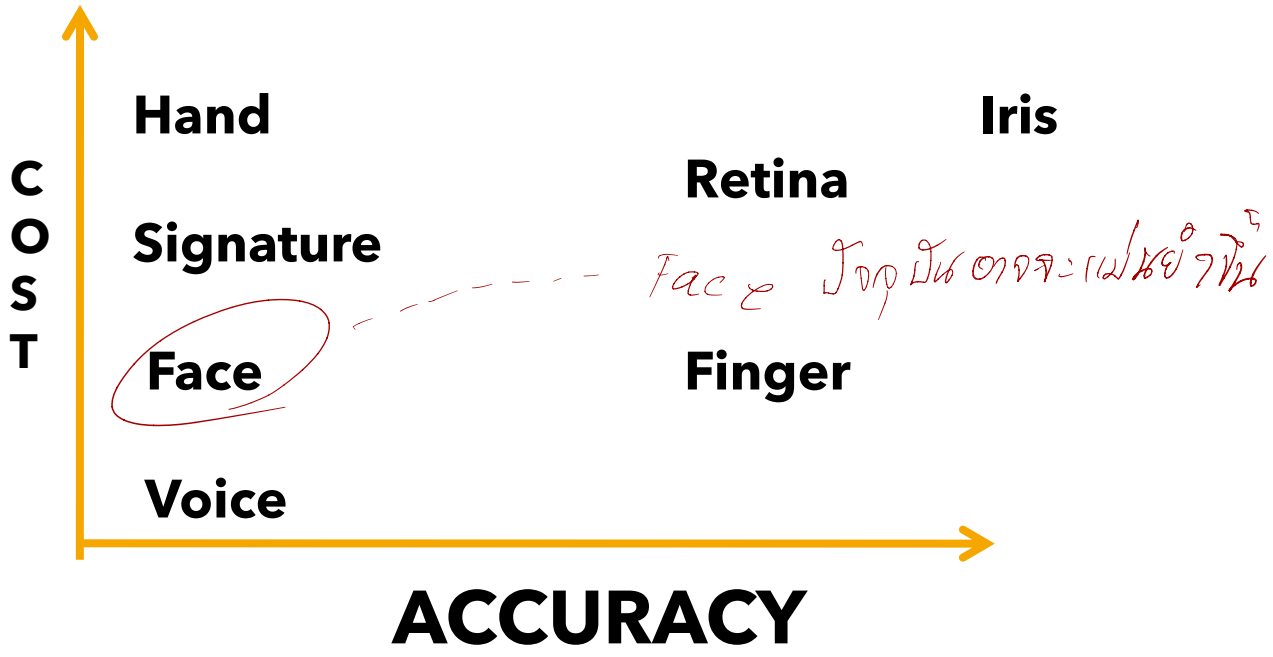
ถ่ายหน้ามาเพื่อทำ extract ได้
machine learning + image processing

พระเอกกับนางเอกหน้าไม่เหมือนกัน

capture , finger print scanner
implement แล้วแพง , ยังเป็น challenging อยู่ ปี 2022

Common characteristics used in Biometric-Application

- Static characters
  - Facial characteristic
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
- Dynamic characters
  - Signature
  - Voice



Something is changed now Guess what

Facial Characters

ไปดูซีรีส์จีน , จีน copy ก่อน, คนจีนเก่งมะคะ
โดนจีนด่า เจ็บจี๊ดดด

- Most common means of human-to-human identification
- Common approach
  - Defining characteristics based on relative location and shape of key facial features
    - Eyes, eyebrows, nose, lips and chin
- Alternative approach
  - Use an infrared to produce face thermogram that correlates with the underlying vascular system in the human faces.

ไม่เวิร์คกับ ศัลยกรรม ;)

Fingerprints, Hand geometry, Retina patterns and Iris

- Fingerprints
  - Is the pattern of rigdes (สัน) and furrows (ร่อง) on the surface of the fingertip.
- Hand geometry
  - Features of hand such as shape, lengths and widths of fingers
- Retinal pattern
  - Use the pattern formed by veins beneath the retinal surface
  - An image of this retinal pattern can be obtained by projecting a low-intensity beam of visual or infrared light into the eyes.
- Iris (รูม่านตา)
  - Use the detail structure of the iris (coz it's unique)

Retinal เยื่อชั้นในของลูกตา

Biometric Authentication System operations:

1.Enrollment

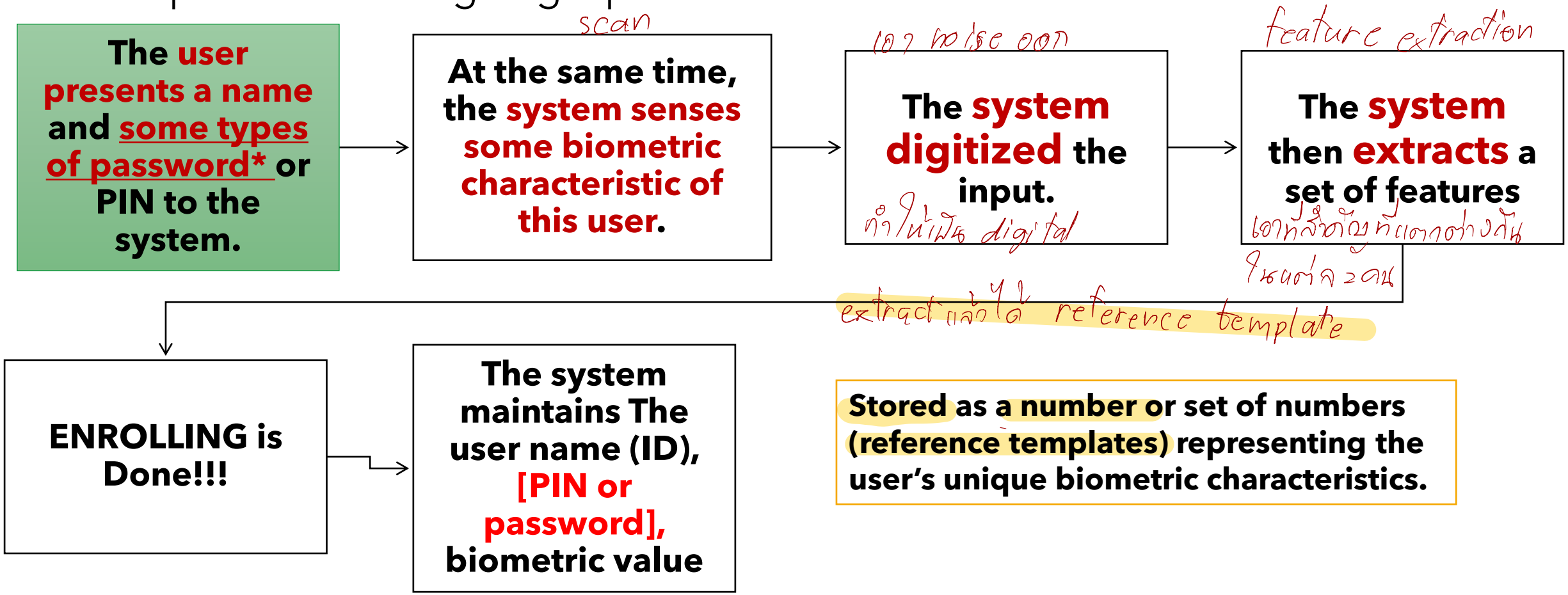
2.Identification

3.Verification

- Biometrics ถูกใช้เพื่อสองวัตถุประสงค์ :[5]
  - Identification: ใช้ identify ว่าเป็น user ในกลุ่มที่อนุญาตให้เข้าถึง
    - 1:*n* comparison
    - tries to identify the user from a database of *n* persons.
  - Verification: ใช้ในการเช็คว่าเป็น user คนนั้นจริงๆ
    - 1:1 comparison
    - checks whether there is a match for a given user.
- Hence, three operations are involved

Biometric Authentication System operation:
1. Enrollment

- Equivalent to assigning a password to a user work as follows:



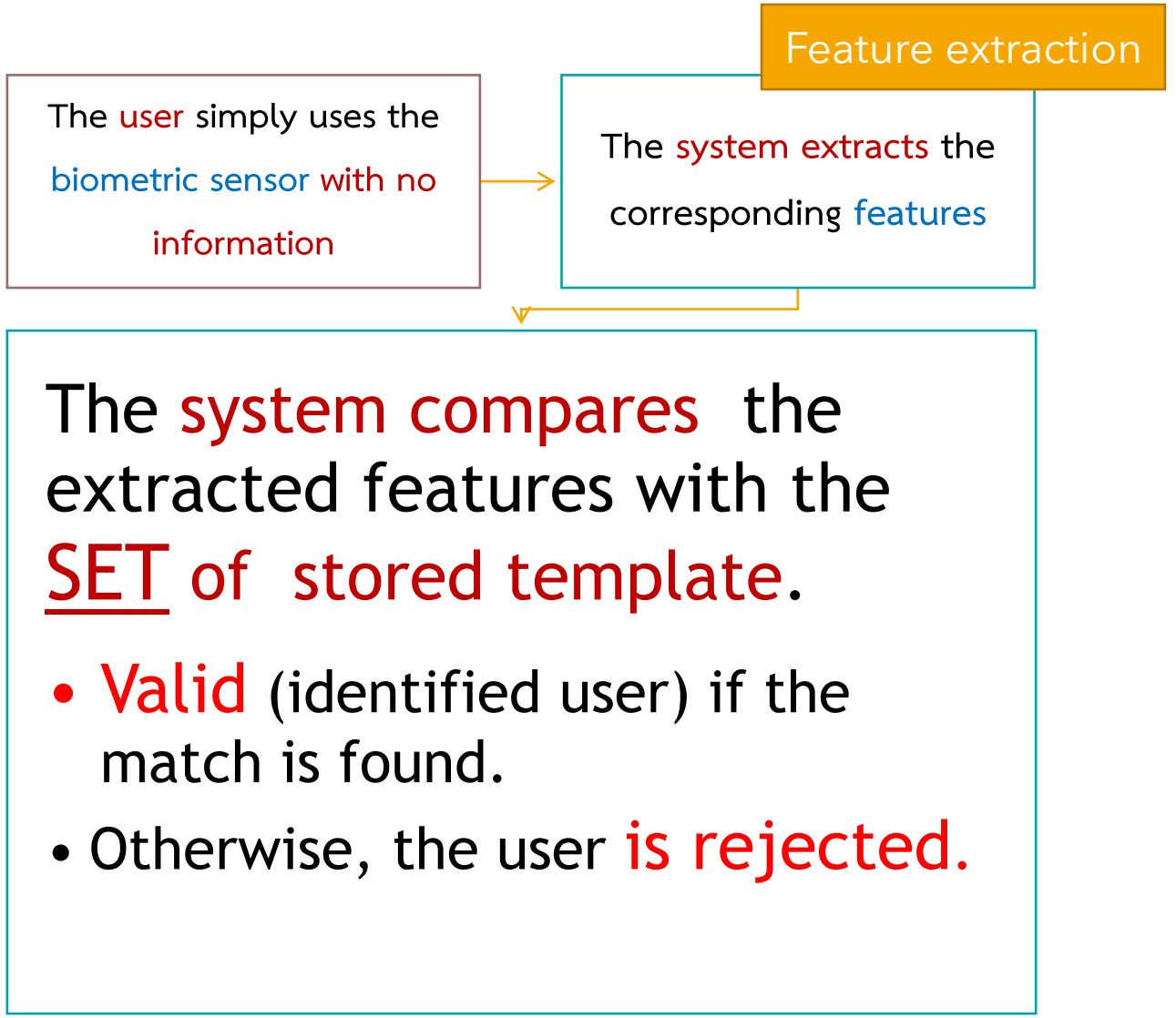
*กรณีที่ใช้ในการ **verify** ต้องมี ถ้าใช้แค่ **identify** ไม่ต้องมี

Example: Fingerprint Enrolment

- Enrolment: A reference template of the user's fingerprint is acquired at a fingerprint reader.
- Failure-to-enrol (FTR): not every person has usable fingerprints.
- For higher accuracy, several templates may be recorded, possibly for more than one finger
- Templates are stored in a secure database.
- When the user logs on, a new reading of the fingerprint is taken and compared against the reference template.

Biometric Authentication System operation:

Enrollment: Identification



Identification does not need any extra information

Biometric Authentication System operation: Enrollment: Verification

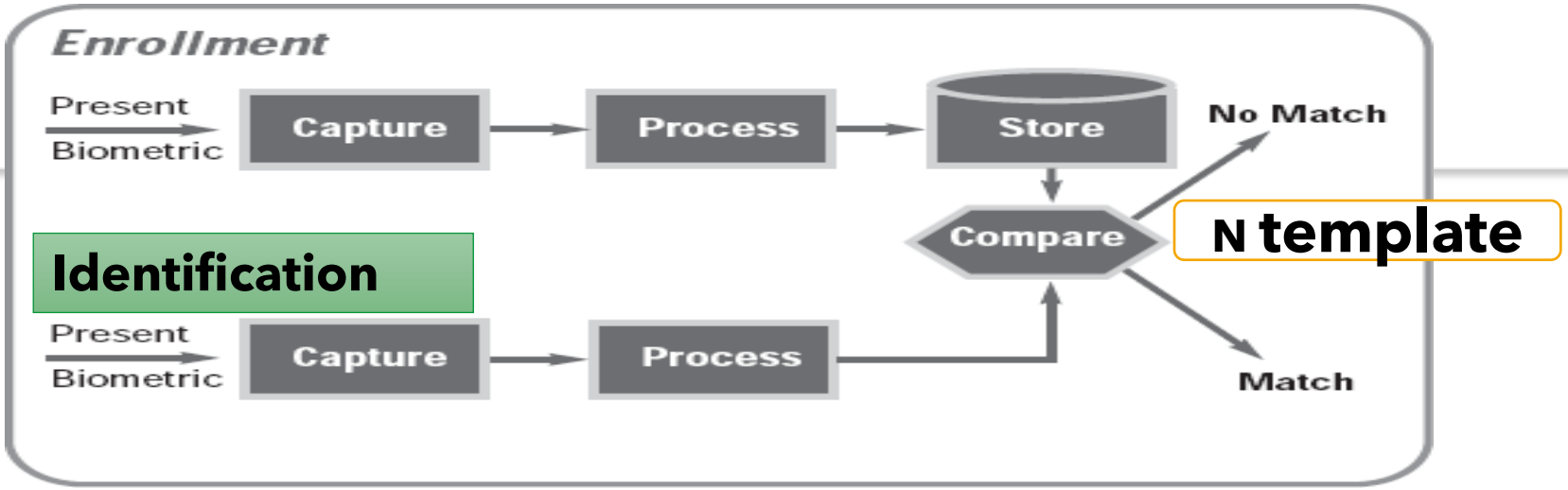
the user enters the PIN and also uses the biometric sensor.

The system Extracts the corresponding features

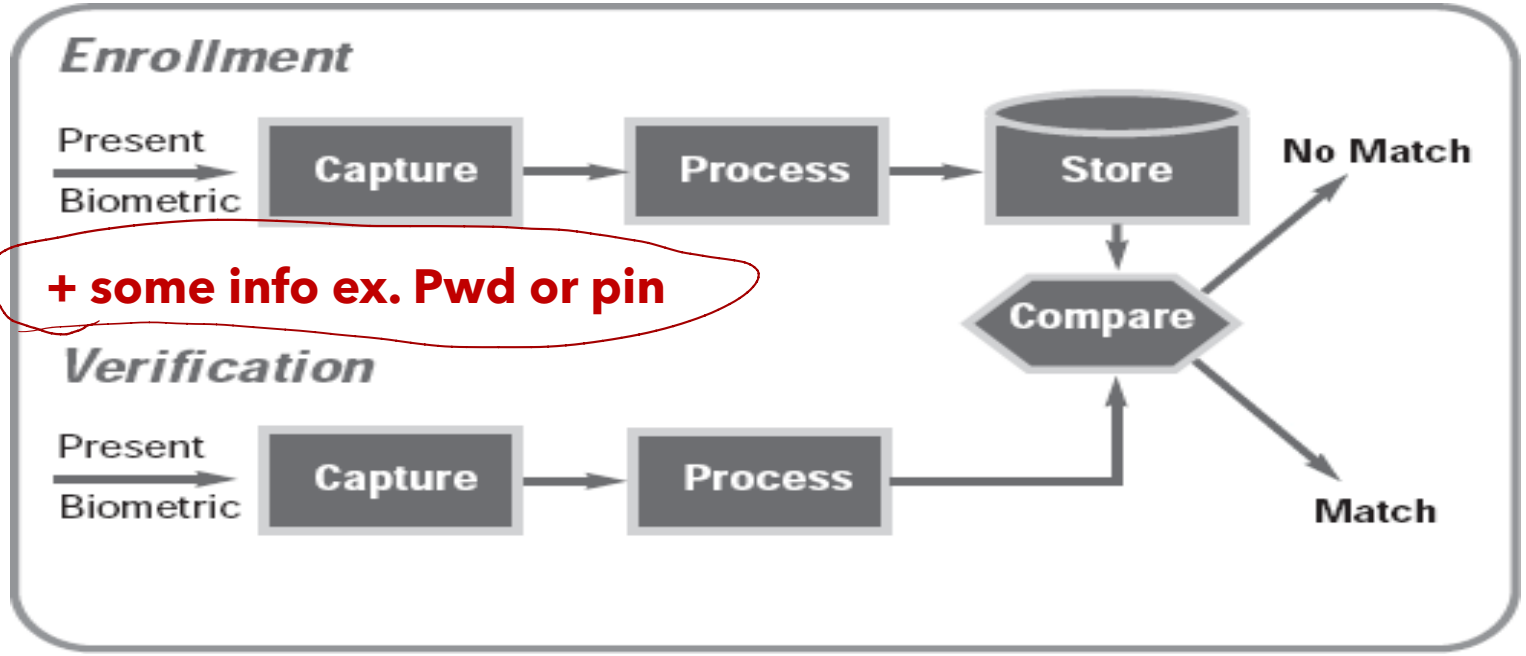
The System Compares the extracted **feature with the user's template**

- **Authenticate if these two are matched.**
- **Reject if they are not**

Similar to the way the user logs into the system using smart card and PIN number.



2 factors



Verification

Books google

Securing Biometrics Applications

books.google.co.th/books?id=QZdpKFFPU8sC&pg=PA2&dq=token+based+authentication&hl=en&sa=X&ved=2ahUKEwjdwIr0pM...

Paused

Google token based authentication

Sign in

Books

Add to my library | Write review | Page 9

Result **1** of **3** in this book for **token based authentication** - ‹ Previous Next › - View all | Clear search

BUY EBOOK - THB 2,449.36

Get this book in print ▼

0 Reviews
Write review

Securing Biometrics Applications

By Charles A. Shoniregun, Stephen Crosier

token based authentica | Go

About this book

My library

My History

Books on Google Play

Terms of Service

Springer

characteristics. This data is then studied by mathematical and statistical methods. In information technology these methods are being used to develop identification methods for biological traits such as fingerprints and retinal scans, to aid in authentication of the user to increase the levels of security that can be achieved. The following diagram (see Figure 1–2 for diagrammatic illustration) shows a generic model of a biometric system, showing the stages, which have to be gone through to get a final decision.

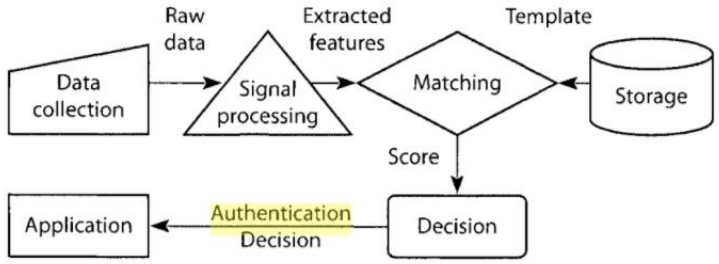


Figure 1–2. Generic biometric system model

The biometric systems are used to 'verify' or to 'identify' an individual. To verify an individual's identity a 1:1 check is made between the biometric data

Securing Biometrics Applications

books.google.co.th/books?id=QZdpKFFPU8sC&pg=PA2&dq=token+based+authentication&hl=en&sa=X&ved=2ahUKEwjdwIr0pM...

Paused

Google token based authentication

Sign in

Books

Add to my library | Write review | Page 6

Result **1** of **3** in this book for **token based authentication** - ‹ Previous Next › - View all | Clear search

BUY EBOOK - THB 2,449.36

Get this book in print ▼

0 Reviews
Write review

Securing Biometrics Applications

By Charles A. Shoniregun, Stephen Crosier

token based authentica | Go

About this book

My library

My History

Books on Google Play

Terms of Service

Springer

Pages displayed by permission of Springer. Copyright.

during enrolment (see Figure 1–1 for diagrammatic illustration). For any biometric system to be effective the data should be stored securely and not be vulnerable to theft, abuse or tampering. The data should also be free of errors to prevent false positive and negative results, and the user must be confident that the system is reliable and secure.

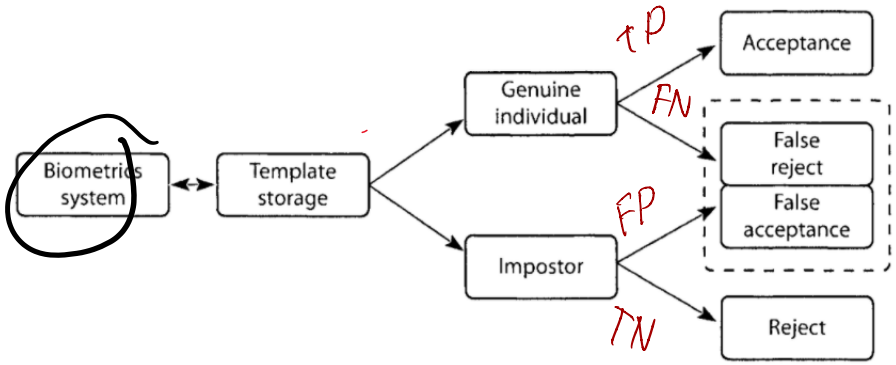


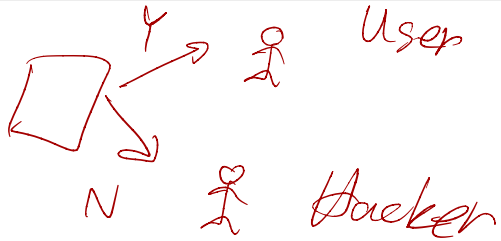
Figure 1–1. Generic biometric system process

The vast amount of data that is now held on everyone and the increases forecast for the future means that it is conceivably possible for people whereabouts to be traced through their use of information. With the need to combat the increasing problems related to identity theft and other security issues, the society will have to make a choice between security and personal freedoms

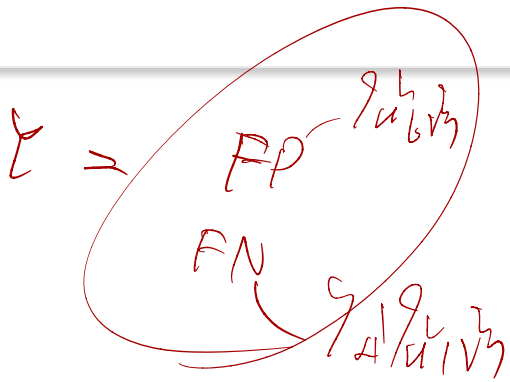
Biometric Authen specific technical problems[5]

- Authentication by password: clear reject or accept at each authentication attempt.
- Biometrics:
  - the stored reference template will hardly ever match precisely template derived from the current measurements.
  - Solution:
    - The similarity between reference template and current template is measured.
    - The user is accepted if the match is above a predefined threshold.
- New issue: **false positives and false negatives**

Failure Rate [5]

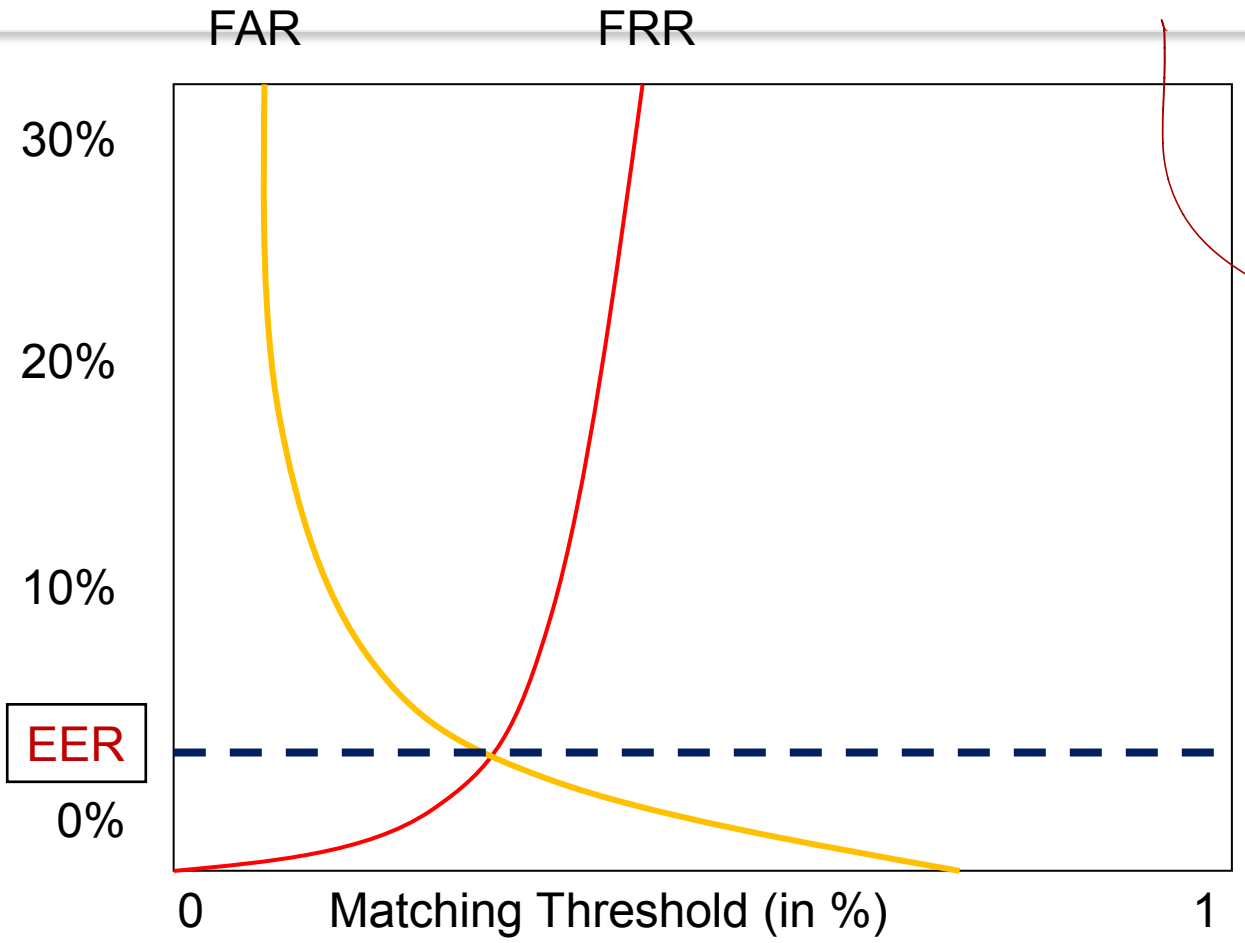


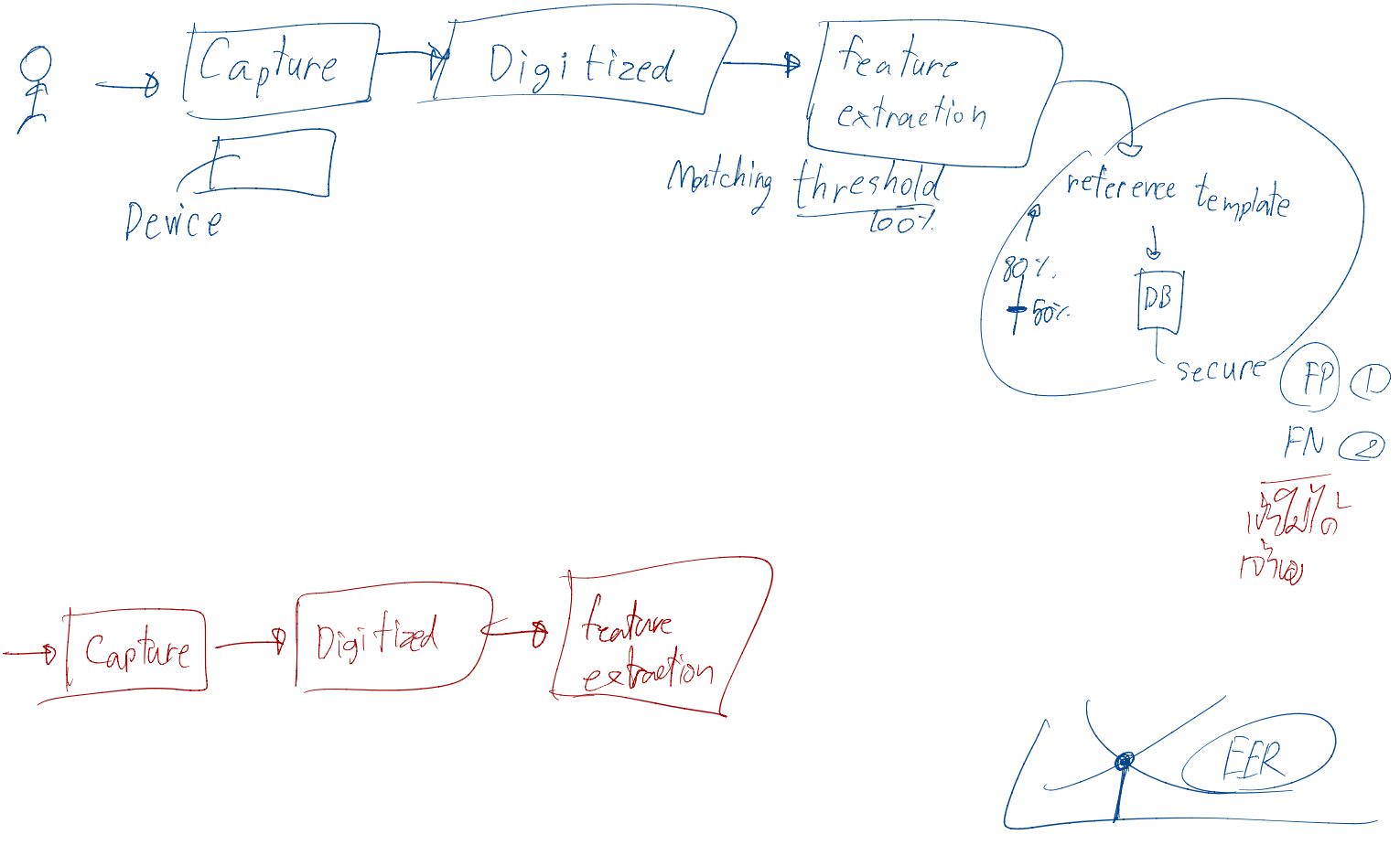
- FP: Accepting the wrong user
  - is a security problem.
- FN: Rejecting a legitimate user
  - creates embarrassment and an inefficient working environment



- By setting the threshold for the matching algorithm, we can trade off a lower false acceptance rate (FAR) against a higher false rejection rate (FRR).
- Finding the right balance between those two errors depends on the application.
- The equal error rate (EER) is given by the threshold value where FAR and FRR are equal.
  - Currently, the best state-of-the-art fingerprint recognition schemes have an EER of about 1-2%.

FAR, FRR, EER




Capture
Digitized
feature extraction
Device
Matching threshold
100%
reference template
80%
50%
DB
secure
FP 1
FN 2
Capture
Digitized
feature extraction
EER

Problems with Biometrics

โดนตีหัวหล้วแสกน

- People resists biometric
- Biometric recognition devices are costly.
  - Installing every user's workstation with a reader can be expensive for a large company with many employers
- If anything happens to what is used as biometric, the accuracy maybe reduced since the all readers use sampling and establish threshold for a match.
  - Voice is affected by an infection
  - User presses one side of a finger more than another.
- Biometrics can become a single point of failure
- False reading is still there.
  - 'If my credit card fails to register, I can always pull out a second card, but if my fingerprint is not recognized, I have only that one finger'
- The speed at which a recognition must be done limits accuracy
- Forgery are possible.
  - An artificial fingerprint produced by researchers in Japan (the jelly baby trick)

Some remarks .

- Fingerprints, and biometric traits may be unique but they are no secrets (not private) ลายนิ้วมือ หรือ biometric อื่น unique จริง แต่ว่า เราทิ้งรอยนิ้วมือไว้ทุกที่
- Rubber fingers that defeat most commercial fingerprint recognition systems can be fabricated quite easily.
  - If authentication takes place in the presence of security personnel this would be a minor issue.
  - When authenticating remote users additional precautions have to be taken to counteract this type of fraud.
- iPhone fingerpring hacking https://www.youtube.com/watch?v=baio0qUj2Lk
- **Fingerprints Can Be Stolen From Online Photos** Facebook
  - https://web.facebook.com/Vocativ/videos/1457129867632577

- Therefore, biometrics tend to most reliable where the use is supervised, by a guard perhaps, and biometrics are there to assist not replace the guard.[2] ไบโอเมตริกซ์เชื่อถือได้เมื่อมีคนเช็คการใช้งานอยู่ด้วย (มีไว้เพื่อช่วยเจ้าหน้าที่รักษาความปลอดภัย ไม่ได้มีไว้แทน)
- Biometrics are generally used to make attacks by outsiders more difficult, and probably more expensive.
- In conclusion: biometrics for authentication should only ever be used as a component of a multi-factor authentication system. [2]
- ดังนั้น เช่นเดียวกับ token ไบโอเมตริกซ์ควรใช้ร่วมกับแฟคเตอร์อื่น

Multiple factor authentication

3FA , 2FA , MFA

- Rather than use one factor, such as a password, we can use multiple factors.
- Generally the different types of authentication have different advantages and disadvantages that can be advantageously combined, or combined to the detriment of security.

Two-factor authentication

- Rather than rely on a single password, two-factor authentication systems use a password or PIN and a device (card or calculator) which is able to provide one-time type passwords.
- For example, consider you want to connect to your bank:
  - You might enter the PIN number into your device and it gives you a one-time login code.
  - Or, you enter the PIN number and the displayed value on the card.
- We will firstly look a special case, "two-factor authentication" which is a name reserved for a special type of pairing, not simply any two factors

From Wikipedia

Smart Tokens [Categorised into three *dimensions*

Physical characteristics

- The smart token will include an embedded microprocessor.
- A smart card - the token that looks like a bank card.
- Or they can look like calculators, keys or other small portable objects.

Interface

- Manual interface: a keypad and display for human/token interaction
- Electronic interface: communicate with a compatible reader/writer

Authentication protocol:

Four types of token devices

- Static tokens
- Synchronous dynamic password generator tokens
- Asynchronous dynamic password generator tokens
- Challenge-response tokens

Type of smart token devices [3]

Static

- Offer a physical means to provide identity
- Require an additional factor to provide authentication
  - Such as password or biometric (this information is stored in the token)

Synchronous dynamic password generator tokens

- Generate a unique password at fix time interval
- This password is entered into the system for **authentication**
- **Clocks on the computer systems and the token must be synchonised**

Type of smart token devices (Cont.)

Asynchonous dynamic password generator tokens

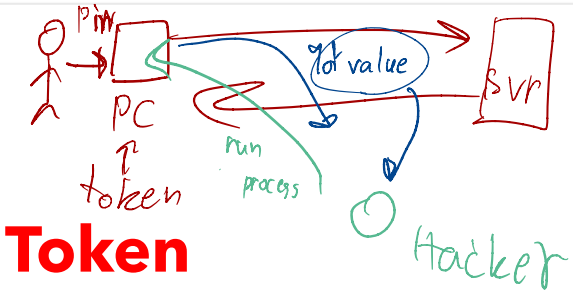
- Generate a unique password based on the occurrence of the event.

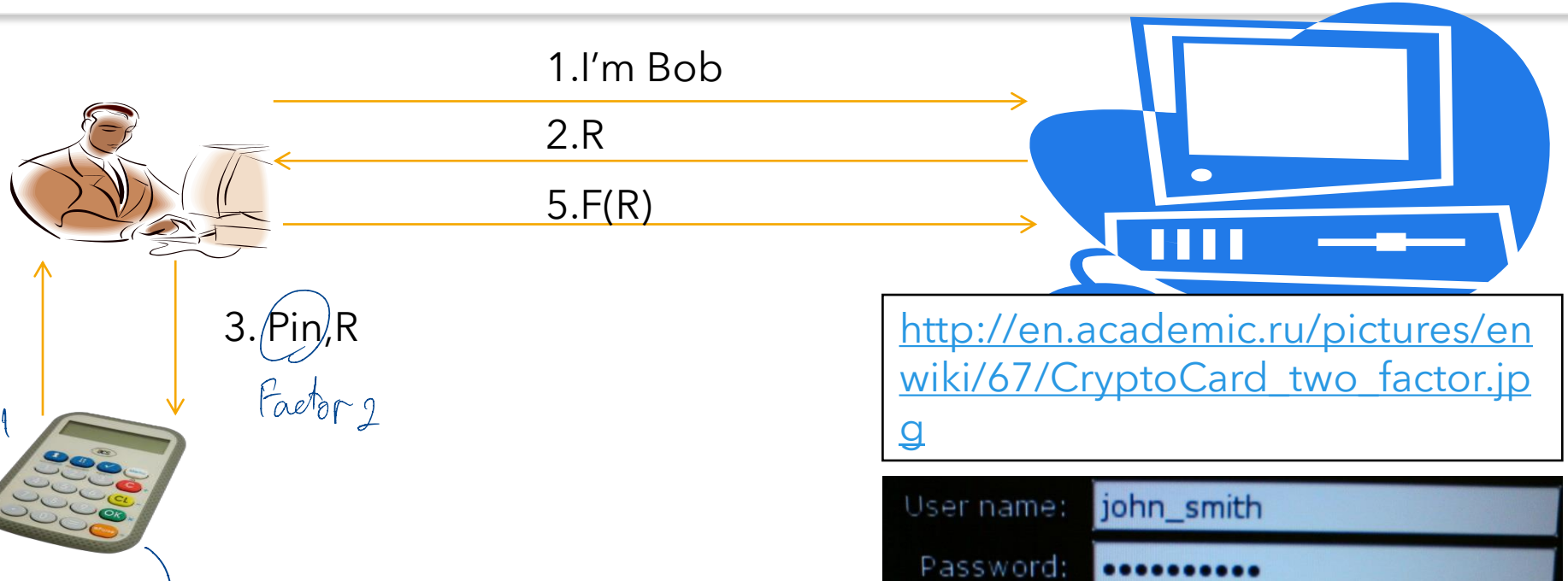
Challenge-response tokens

- The computer system generates a challenge such as a random strings of number
- The challenge is entered to the smart token.
- The smart token generates responses based on that challenge
- The response is entered into the system for authentication.

เพิ่มเติม ตย Smart Token in TFA

Challenge-Response Token

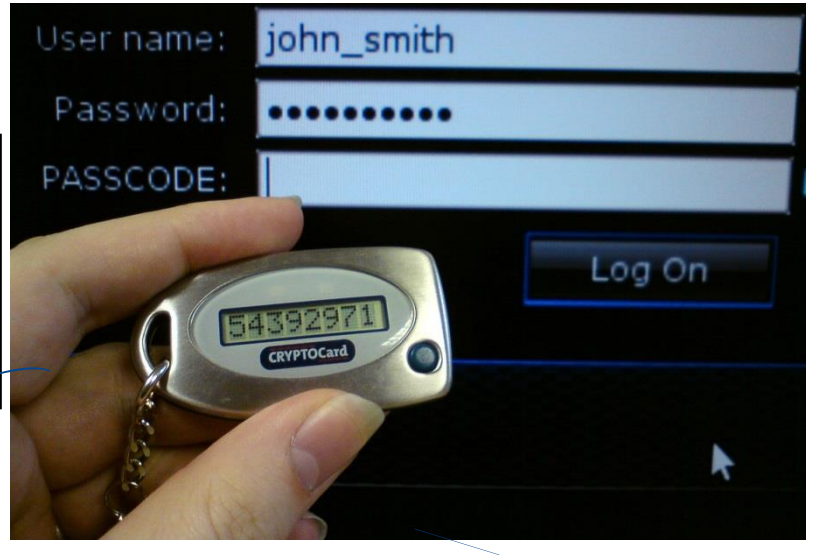




http://en.academic.ru/pictures/enwiki/67/CryptoCard_two_factor.jpg

Disconnected token

Synchronous dynamic password generator tokens



Hard Tokens (Physical)

1 Device → Factor เดียว แต่ 2 steps / 2 state verification

Schneier on two-factor authentication

- Schneier has some interesting things to say about two-factor authentication:
  - It solves the problem of eavesdropping and offline password attacks.
  - It doesn't address the current real problems:
    - Trojan horses.
    - Phishing.
    - We will look at both of these later in the subject.

http://www.schneier.com/blog/archives/2005/03/the_failure_of.html

ดารา Holywood ใช้ password Apple ห่วย

ฝืนเดาน่ะ

Two-step verification [wiki]

- Simple case of multi-factor
- อาจจะประกอบไปด้วย แฟคเตอร์เดียว สองแฟคเตอร์ หรือ มากกว่า แต่ทำสองขั้นตอน
- กูเกิลเป็นองค์กรแรกๆ ที่นำวิธีการนี้มาใช้
  - Step 1 : Login ด้วย username กับ password ก่อน
  - Step 2 :
    - แบบที่ 1 : Google จะ SMS โค้ด มาทางโทรศัพท์มือถือ ที่ผู้ใช้ต้อง ลงทะเบียนเบอร์ไว้ (เหมือน TFA เพราะจะมี code นี้ได้ ต้องมีโทรศัพท์ (sth we have)
    - แบบที่ 2 : ใช้ Google Authenticator application ใช้แอพในการ gen authenticator code (แทนที่จะใช้ token) (กรณีนี้ factor เดียว แต่ two step)
      - แอพต้องมีการ set up key ที่ใช้ gen auth code กับเว็บ เช่น กรณีนี้ คือ กูเกิลก่อน
- https://www.google.com/landing/2step/index.html#tab=how-it-protects

Google Authenticator Code*

```
function GoogleAuthenticatorCode(string secret)
    key := base32decode(secret)
    message := floor(current Unix time / 30)
    hash := HMAC-SHA1(key, message)
    offset := value of last nibble of hash
    truncatedHash := hash[offset..offset+3]  //4 bytes starting at the offset
    Set the first bit of truncatedHash to zero  //remove the most significant bit
    code := truncatedHash mod 1000000
    pad code with 0 until length of code is 6
    return code
```

แบบใช้ time

```
function GoogleAuthenticatorCode(string secret)
    key := base32decode(secret)
    message := counter encoded on 8 bytes
    hash := HMAC-SHA1(key, message)
    offset := last nibble of hash
    truncatedHash := hash[offset..offset+3]  //4 bytes start
    Set the first bit of truncatedHash to zero  //remove the
    code := truncatedHash mod 1000000
    pad code with 0 until length of code is 6
    return code
```

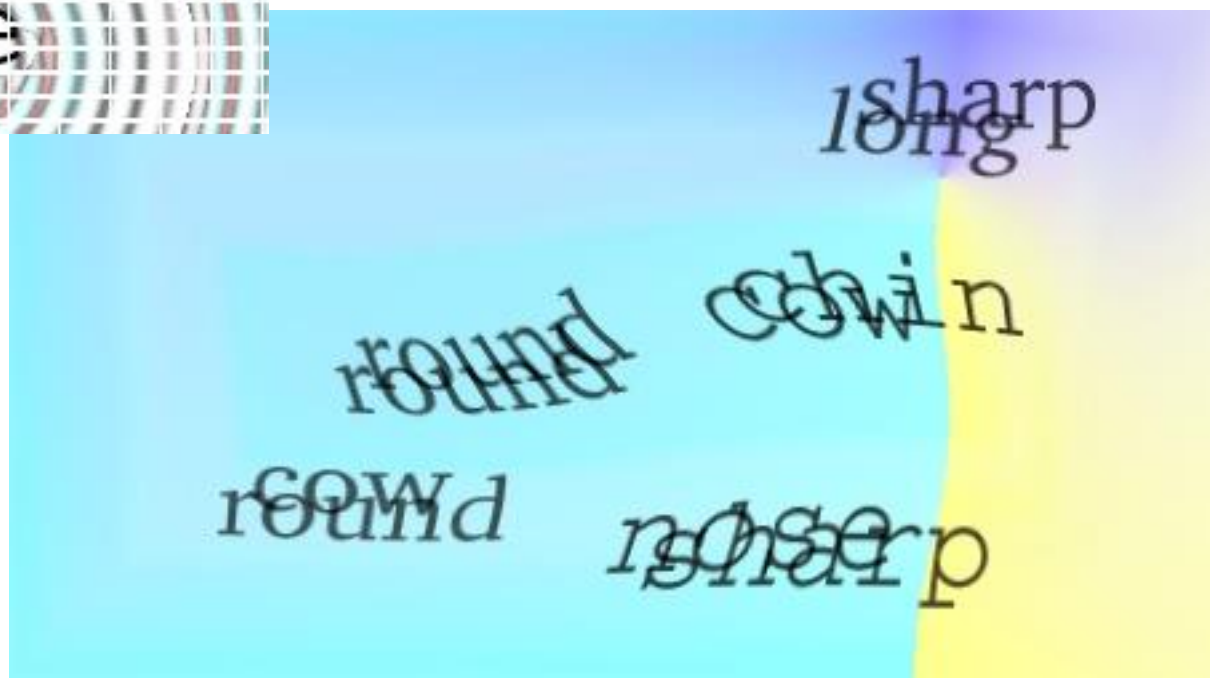
แบบใช้ event หรือ counter

**http://en.wikipedia.org/wiki/Google_Authenticator

CAPTCHA

ครูโอ๋ ใช้แต่ไทยพาณิชย์ , กสิกรเจ๋งอ่ะ อยู่ที่เดียวกันตลอดเป็น
เป๋าตังเก่งขึ้นใช้ GPS

- Completely Automated Public Turing Test to Tell Computers and Humans Apart.
- It exploits the human ability to correct distortions in images, and generally perform image recognition, far better than existing automated systems.
- It has uses in authentication and in denial of service.
  - Denial of service is somewhat related to authentication and will be discussed later.



Computer algorithms aren't as good at recognising such distorted words as we are.

CAPTCHA Cont.

มันเก่งนะเนี่ย , Google มันเก่ง

- The idea is that only humans can easy read the content of the distorted message.
  - There are also audio versions.
- So, we declare something to be human if it can read one, or often a series of images.
- For authentication we can imbed a challenge to make the response a function of the entity being authenticated.
  - For example, the image could tell you to enter 1452522 into your key calculator and reply with the output.
  - The key calculator is "keyed" to you.

References:

- [1] CSCI262 Lecture Notes by Dr. Luke McEvan, University of Wollongong Australia.
- [2] Leslie Lamport, Password authentication with insecure communication, Communications of the ACM, v.24 n.11, p.770-77
- [3] Computer Security: Principles and Practice, W. Stalling and L. Brown, 1st edition, Pearson Education, 2008.
- [4] Security in Computing, C.P. Pfleeger and S.L. Pfleeger, 4th edition, Prentice Hall, 2007.
- [5] Computer Security, D. Gollman. 2nd edition, John Wiley & Sons, 2006.
- [6] Wikipedia.org
- https://www.wired.co.uk/article/password-cracking

List of videos

- Double Blind Password
  - https://youtu.be/boj9q26gadE
- 2 step verification from google
  - https://www.youtube.com/watch?v=zMabEyrtPRg
- TFA
  - https://www.youtube.com/watch?v=QLQHHScn0yA
- RSA Secure ID
- Yubi Key
  - https://www.youtube.com/watch?v=W7if0FW12D0
  - https://www.youtube.com/watch?v=NhgJwVQT7NM

กลุ่มละ 2 คน

1. NIST Password Guide ให้หนูไปศึกษาและสรุปมา
2. The Best Facial Recognition Algorithm .. คือ และ Accuracy อยู่ที่เท่าไหร่