

COSC 362

Chapter 3. User Authentication



Means of Authentication

§ Something the individual knows

- Password, PIN (Personal Identification Number), or answers to a prearranged set of questions

§ Something the individual possesses (tokens)

- Electronic keycards, smart cards, physical keys, ...

§ Something the individual is (static biometric)

- fingerprint, retina, face, ...

§ Something the individual does (dynamic biometric)

- voice pattern, handwriting characteristics, and typing rhythm



Password Vulnerabilities

Google most popular passwords of all time

전체 이미지 동영상 뉴스 지도 더보기 설정 도구

검색결과 약 10,900,000개 (0.51초)

The world's most common passwords revealed: Are you using them?
www.telegraph.co.uk/Technology/ 이 페이지 번역하기
2017. 1. 16. - More than 50pc of people use the top 25 most common passwords, according to password manager Keeper, with a significant 17pc - almost one in five - of all users having "123456" as their protective code. Keeper compiled the list by scouring 10 million passwords leaked in data breaches. Predictably, the ...

PasswordRandom.com - Top 10000 most common passwords list ...
www.passwordrandom.com/most-popular-passwords/ 이 페이지 번역하기
Top 10000 most common passwords used on the Internet: 91% of all profile passwords sampled all appear on the list of just the top 1000 passwords. ... Why bother to create each time new passwords and keep them in mind. If there is a necessity to log on ... As a matter of fact, you don't need remember all your passwords.

What the Most Common Passwords of 2016 List Reveals [Research ...]
[https://blog.keepersecurity.com/.../most-common-passwords-of-2...](http://blog.keepersecurity.com/.../most-common-passwords-of-2...) 이 페이지 번역하기
2017. 1. 13. - Looking at the list of 2016's most common passwords, we couldn't stop shaking our heads. Nearly 17 percent of ... While it's important for users to be aware of risks, a sizable minority are never going to take the time or effort to protect themselves. ... After all, it's in the user's best interests to do so. But the ...

List of the most common passwords - Wikipedia
[https://en.wikipedia.org/.../List_of_the_most_common_passwords](http://en.wikipedia.org/.../List_of_the_most_common_passwords) 이 페이지 번역하기
This is a list of the most common passwords, according to various sources. Common passwords generally are not recommended on account of low password strength. Contents. [hide]. 1 List. 1.1 SplashData; 1.2 Keeper. 2 See also; 3 Notes; 4 References; 5 External links. List[edit]. SplashData[edit]. The Worst Passwords ...
List · SplashData · Keeper

The 25 Most Popular Passwords of 2017: You Sweet, Misguided Fools
[https://gizmodo.com/the-25-most-popular-passwords-of-2017-ye...](http://gizmodo.com/the-25-most-popular-passwords-of-2017-ye...) 이 페이지 번역하기
2017. 12. 19. - Every year, SplashData compiles a list of the most popular passwords based on millions of stolen logins made public in the last year. And each time, we own ourselves. Hard. 2017 is no exception. ... The 25 Most Popular Passwords of 2015: We're All Such Idiots ...

The Top 500 Worst Passwords of All Time | Symantec Connect ...
[https://www.symantec.com/.../top-500-worst-passwords-all-time](http://www.symantec.com/.../top-500-worst-passwords-all-time) 이 페이지 번역하기
2010. 4. 13. - Do you think your password is unique in the world? Please take some minutes to read the The Top 500 Worst Passwords of All Time. Many interesting information are shown in this article, for example do you know that the all time most.



Top 25 most common passwords

- | | | |
|----|------------|---------------|
| 1 | 123456 | |
| 2 | 123456789 | 16 7777777 |
| 3 | qwerty | 17 lq2w3e4r |
| 4 | 12345678 | 18 654321 |
| 5 | 111111 | 19 555555 |
| 6 | 1234567890 | 20 3rjslla7qe |
| 7 | 1234567 | 21 google |
| 8 | password | 22 lq2w3e4r5t |
| 9 | 123123 | 23 123qwe |
| 10 | 987654321 | 24 zxcvbnm |
| 11 | qwertyuiop | 25 lq2w3e |
| 12 | mynoob | |
| 13 | 123321 | |
| 14 | 666666 | |
| 15 | 18atcskd2w | |

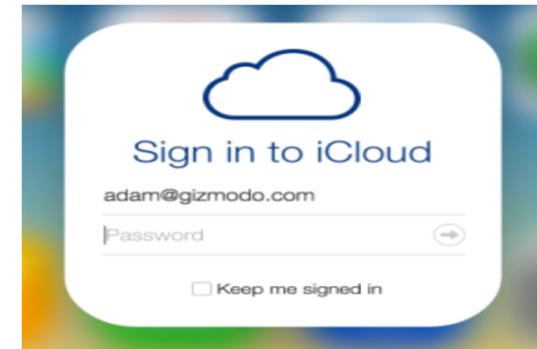
Passwords Cracked from a Sample Set of 13,797 Accounts

Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio ^a
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths and legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

*Computed as the number of matches divided by the search size. The more words that need to be tested for a match, the lower the cost/benefit ratio.

*Stallings and Brown, Table 3.2

Always Happening



Same old story...

Cyber-Safe

Google says hackers steal almost 250,000 web logins each week

by Selena Larson @selenalarson

Nov 9, 2017: 4:13 PM ET



CNN tech

All Control Panel Items > Windows Update

Windows Update

Download and install updates for your computer

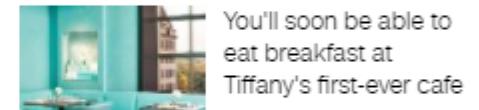
8 important updates are available
5 optional updates are available

7 important updates selected, 304.7 MB
- 304.8 MB

Install updates

Most recent check for updates: Today at 14:34
Updates were installed: 07/06/2017 at 11:08. [View update history](#)
You receive updates: Managed by your system administrator

How to protect yourself from hackers



Google is digging into the dark corners of the web to better secure people's accounts.

SEC hands down \$35 million fine in Yahoo hack

by Heather Kelly @heatherkelly

🕒 April 24, 2018: 5:28 PM ET



The image shows a 'WANTED BY THE FBI' poster featuring two men. On the left is Dmitry Aleksandrovic, and on the right is XVD. The background is a blurred image of a building at night.

DOJ: Russian agents behind Yahoo cyberattack

Yahoo may have changed its name, but it's still paying for a massive 2014 data breach.

Altaba, what's left of Yahoo after the company sold most of its properties, has agreed to pay \$35 million to settle charges that it misled investors about the hack, the US Securities and Exchange Commission said Tuesday.

In 2017, Yahoo completed the sale off its core business to Verizon for \$4.48 billion. It retained large stakes in e-commerce company Alibaba and Yahoo Japan and changed its name to Altaba.

IT 담당자가 없어 네트워크 구축에 고민인 중소 중견기업을 위해 시스코 START가 고민을 해결해 드립니다.

확인하기 >

Cisco Start

Advertisement

Investing

Take Control of Your Future Today

ally INVEST

Brokerage Account

Get 90 days of commission-free trading or \$200 cash!

Open Account

TD Ameritrade

IRA

Get up to \$2,500 when you roll over your old 401k into a TD Ameritrade IRA.

Open Account

E*TRADE

Brokerage Account

\$6.95 online equity and options trades

Open Account

Sponsors of GO BankingRates

Advertiser Disclosure

Paid Content

by Outbrain ▶

China's Youngest Female Billionaire



No surprise at all

john the ripper

All Videos Images News Books More Settings Tools

About 785,000 results (0.36 seconds)

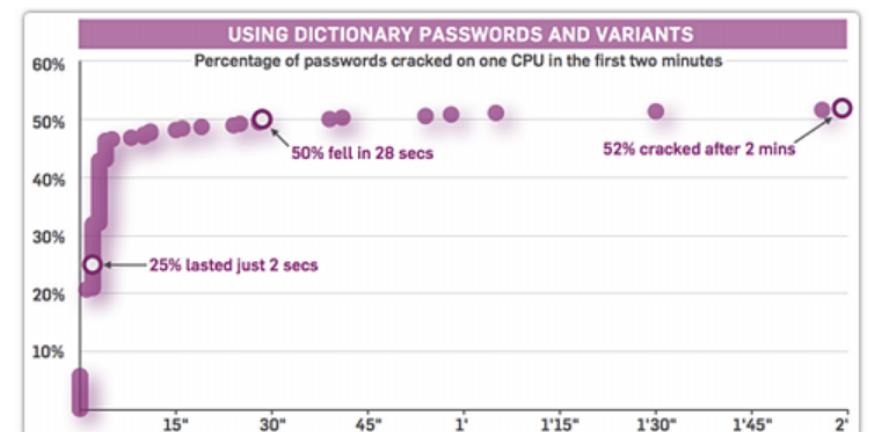
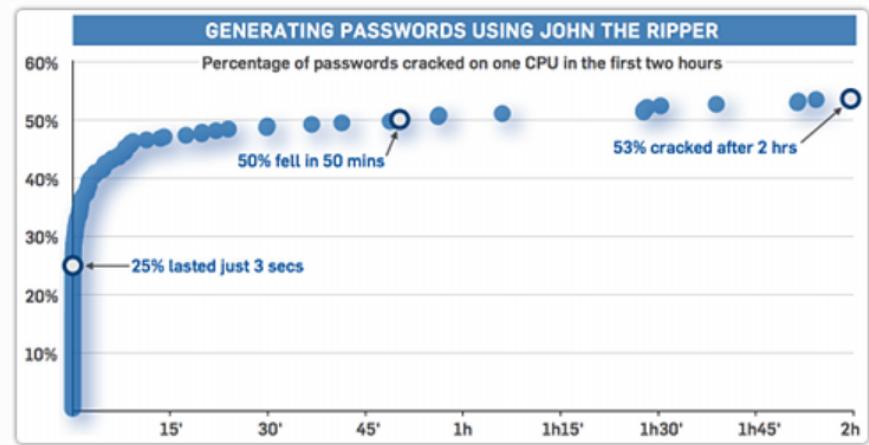
John the Ripper password cracker - Openwall
www.openwall.com/john/ ▾
A fast password cracker for Unix, Windows, DOS, and OpenVMS, with support for Unix, Windows, and Kerberos AFS passwords, plus a lot more with contributed patches.

John the Ripper Pro
John the Ripper Pro password cracker. John the Ripper is a ...
More results from openwall.com »

John the Ripper - Wikipedia
https://en.wikipedia.org/wiki/John_the_Ripper ▾
John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms. It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and ...
Sample output · Attack types

GitHub - magnumripper/JohnTheRipper: This is the official repo for the ...
https://github.com/magnumripper/JohnTheRipper ▾
GitHub is where people build software. More than 27 million people use GitHub to discover, fork, and contribute to over 80 million projects.

John the Ripper – SecTools Top Network Security Tools
sectools.org/tool/john/ ▾
John the Ripper is a fast password cracker for UNIX/Linux and Mac OS X.. Its primary purpose is to detect weak Unix passwords, though it supports hashes for many other platforms as well. There is an official free version, a community-enhanced version (with many contributed patches but not as much quality assurance), ...



(Text-based) Password Vulnerabilities

	How it works	Threats	Potential Countermeasures
Offline dictionary attack			
Specific account attack			
Popular password attack			
Password guessing			
Shoulder surfing (or social engineering)			
Workstation hijacking			
Exploiting user mistakes			
Exploiting multiple password use			
Electronic monitoring			

§ Especially difficult when managing passwords on multiple sites



Password Managers, Single sign-on, ...

- § Is this a good idea?
- § Browsers often perform the role of password managers

Google Search Results for "password managers":

- The Five Best Password Managers - Lifehacker**
https://lifehacker.com/5529133/five-best-password-managers ▾ 이 페이지 번역하기
2017. 8. 22. - A while ago, all it took to be a great password manager was to keep your passwords in an encrypted vault. Now the best password managers give you the option to sync or keep them local only, change web passwords with a click, log in to sites for you, and more.
- The Best Password Managers of 2018 | PCMag.com**
https://www.pc当地/2017/2407168.00.asp ▾ 이 페이지 번역하기
Still using your kid's birthday as your universal password? You're heading toward trouble. With the help of a password manager, you can have a unique and strong password for every secure website. We've evaluated two dozen to help you choose.
LogMeOnce Password ... · The Best Free Password ... · Keeper Password Manager
- The best free password manager and generator 2018 | TechRadar**
www.techradar.com/news/.../the-best-password-manager-132584... ▾ 이 페이지 번역하기
2017. 12. 6. - The best password managers then encrypt and store these passwords in a secured vault that's protected by a master password, meaning you only have to remember one password. Once you're logged into the manager, these programs will automatically fill your username and password each time you visit ...
- You Need a Password Manager. Here Are Some Good Free Ones ...**
https://www.wired.com/2016/01/you-need-a-password-manager/ ▾ 이 페이지 번역하기
2016. 1. 24. - Face it: That whole writing-it-down system isn't really working for you—get a password manager.
- List of password managers - Wikipedia**
https://en.wikipedia.org/wiki/List_of_password_managers ▾ 이 페이지 번역하기
The following is a list of some of the password managers for which there are Wikipedia articles.
Contents. [hide]. 1 Basic Information; 2 Features; 3 References; 4 Bibliography. Basic Information[edit]. Name, License, OS Support, Browser Integration, Delivery Format. 1Password · Proprietary · Android, iOS, macOS, Windows ...

Google Search Results for "single sign on":

- 통합 인증 - 위키백과, 우리 모두의 백과사전**
https://ko.wikipedia.org/wiki/통합_인증 ▾
통합 인증(영어: Single Sign-On, SSO)은 한 번의 인증 과정으로 여러 컴퓨터 상의 자원을 이용 가능하게 하는 인증 기능이다. 싱글 사인온, 단일 계정 로그인, 단일 인증이라고 한다. 예를 들어 어느 컴퓨터에 로그인한 후 그룹웨어 등의 응용 프로그램을 사용할 때에 또 로그인, 다른 서버상의 응용 프로그램을 사용할 때에도 다시 로그인 ...
- Single sign-on - Wikipedia**
https://en.wikipedia.org/wiki/Single_sign-on ▾ 이 페이지 번역하기
Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each ...
- Single Sign On (SSO) with Auth0**
https://auth0.com/docs/ssو ▾ 이 페이지 번역하기
The Hosted Login Page is the easiest and most secure way to implement SSO with Auth0. If you need to use embedded Lock or an embedded custom authentication UI in your application, check out the Cross-Origin Authentication page for information on safely conducting SSO.
- What is single sign-on (SSO)? - Definition from WhatIs.com**
searchsecurity.techtarget.com > ... Network security ▾ 이 페이지 번역하기
2016. 6. 21. - Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts ...
- Enterprise Single Sign-on 구현 - BizTalk Server | Microsoft Docs**
https://docs.microsoft.com/ko-kr/biztalk/core/implementing-enterprise-single-sign-on
2017. 6. 8. - Enterprise SSO(Single Sign-On)는 EAI(엔터프라이즈 응용 프로그램 통합) 솔루션의 최종 사용자가 Single Sign-On을 사용할 수 있는 서비스를 제공합니다. ... SSO 시스템은 Microsoft Windows 계정을 백 엔드 자격 증명에 매핑합니다. ... SSO는 사용자 및 관리자 모두의 사용자 ID 및 암호 관리를 간소화합니다. SSO ...
- Understanding Enterprise Single Sign-On - MSDN - Microsoft**
https://msdn.microsoft.com/en-us/_/aa745042(v=bts.10).aspx ▾ 이 페이지 번역하기
To understand Enterprise Single Sign-On (SSO), it is useful to look at the three types of Single Sign-On services available today: Windows integrated, extranet, and intranet. These are described in the following sections, with Enterprise Single Sign-On falling into the third category.

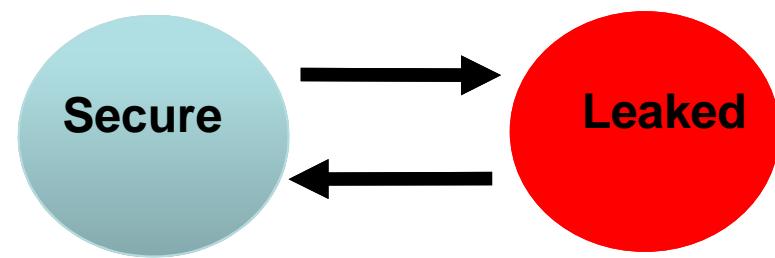


“Personal” Nightmare



§ This list is most likely the tip of the iceberg !

- Very (extremely?) difficult to remember
- Heavily reused, small candidate pools, special character rules, ...
- Difficult, if not impossible, to detect attacks in timely manner
- ...



Personal “trauma”?

한국연구재단 홈페이지에 오신것을 환영합니다.

로그인을 하시면 더 많은 서비스를 이용 하실 수 있습니다.

회원 로그인

[회원가입](#) | [아이디/비밀번호 찾기\(재단회원\)](#) | [아이디/비밀번호 찾기\(기관회원\)](#)

15

1. 본인확인서비스

4,8
PIN)인증(대리인 가능)으로
온라인상에서 주민등록번호!

4,8
PIN)인증(대리인 가능)으로
온라인상에서 주민등록번호!

15

2.6



안심본인인증 본인확인

안심본인인증(대리인 가능)으로 본인확인

안심본인인증 서비스는 본인 명의 휴대폰, 개인용으로 유료 구입한 범용 공인인증서를 이용하여 온라인상에서 본인을 확인하는 서비스입니다.

안심본인인증 실패 관련 고객센터 : NICE평가정보 (☎ 1600-1522)

nice.checkplus.co.kr 내용:

고객님의 안전한 서비스 이용을 위하여
보안프로그램 설치가 필요합니다.
[확인]을 선택하시면 설치페이지로 연결됩니다.

확인

취소



Best Practices for Enforcing Password Policies (Microsoft)

- § Enforce password history
- § Maximum password age
- § Minimum password age
- § Minimum password length
- § Passwords must meet complexity requirements
- § Store password using reversible encryption for all users

The screenshot shows a Microsoft TechNet page with the following details:

- Page Title:** Tip: Best Practices for Enforcing Password Policies
- Page URL:** https://technet.microsoft.com/en-us/library/ff741764.aspx
- Content Summary:** Troubleshoot Group Policy from the Command Line with GPRESULT
- Related Links:**
 - Fix Remote Administration when Windows Firewall Gets in the Way
 - Enable the Print Job Error Notification on Windows Server 2008
 - Best Practices for Enforcing Password Policies** (highlighted in blue)
 - Back Up and Restore the DHCP Database
- Follow Our Daily Tips:**
 - facebook.com/TechNetTips
 - twitter.com/TechNetTips
 - blogs.technet.com/tmag
- Text Block:** No matter how secure you make a user's password initially, she will eventually choose her own password. Therefore, you should set account policies that define a secure password for your systems. Account policies are a subset of the policies configurable in Group Policy. Here's a look at the key settings you will work with.
- Section Header:** Enforce Password History
- Description:** This sets how frequently old passwords can be reused. With this policy, you can discourage users from alternating between several common passwords. Windows Server 2008 R2 can store up to 24



/etc/passwd

<https://en.wikipedia.org/wiki/Passwd>



The `/etc/passwd` file is a text-based database of information about users that may log into the system or other operating system user identities that own running processes.

In many operating systems this file is just one of many possible back-ends for the more general `passwd` name service.

The file's name originates from one of its initial functions as it contained the data used to verify passwords of user accounts. However, on modern Unix systems the security-sensitive password information is instead often stored in a different file using shadow passwords, or other database implementations.

The `/etc/passwd` file typically has file system permissions that allow it to be readable by all users of the system (*world-readable*), although it may only be modified by the superuser or by using a few special purpose privileged commands.

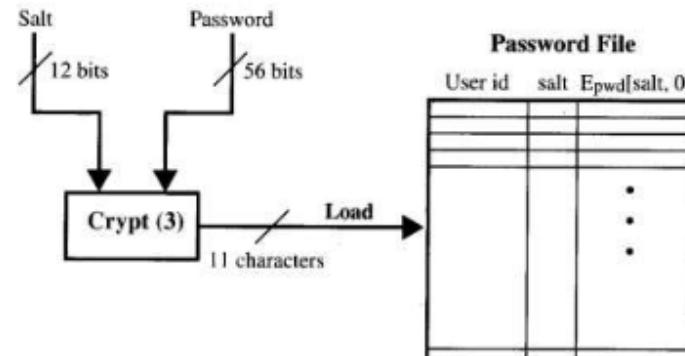
The `/etc/passwd` file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons. The ordering of the records within the file is generally unimportant.

An example record may be:

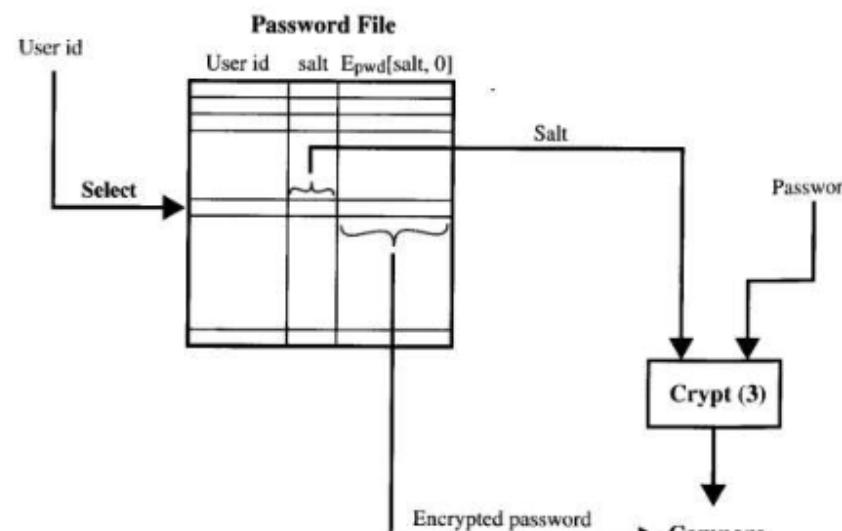
```
jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-  
0044,email:/home/jsmith:/bin/sh
```



UNIX Password Scheme



(a) Loading a new password



(b) Verifying a password

Figure 15.5 UNIX Password Scheme

*Figure 3.1 in Stallings and Brown



(From W. Stallings, Operating Systems)

“Unix salt”

- § It prevents duplicate passwords from being visible in the password file
- § It greatly increases the difficulty of offline dictionary attacks. For a salt of length b bits, the number of possible passwords is increased by a factor of 2^b
- § It becomes nearly impossible to find out whether a person with passwords on two or more systems have used the same password on all of them



/etc/shadow and salt

← → C | 안전함 | <https://superuser.com/questions/822079/etc-shadow-in-old-format-where-is-salt-stored>

/etc/shadow in old format, where is salt stored?

 Microsoft Azure banner: "직접 체험하며 배울 수 있는 기회! 25개가 넘는 서비스가 Azure에서는 항상 무료입니다." with a "Azure 무료 체험" button.

In /etc/shadow I have entries such as `admin:YtChlvAGYZva2:16318:0:99999:7:::`. I know the original password and would like to generate the same hash somehow. However, running `openssl passwd -crypt password` gives me different results every time I run it. I assume salt is involved, so where can I find the salt used to create the original hash?

Edit: I got the original hash using the following command:

`openssl passwd -crypt -salt Yu password`

The salt and the encrypted password are both mashed into the string `YtChlvAGYZva2`.

From the [Shadow Password Howto](#):

When a user picks or is assigned a password, it is encoded with a randomly generated value called the salt. This means that any particular password could be stored in 4096 different ways. The salt value is then stored with the encoded password.

When a user logs in and supplies a password, the salt is first retrieved from the stored encoded password.

The longer password strings you see with modern systems [separate the hash using \\$](#). But for the older systems, it was just mashed in ([Wikipedia](#)):

Earlier versions of Unix used a password file (/etc/passwd) to store the hashes of salted passwords (passwords prefixed with two-character random salts). In these older versions of Unix, the salt was also stored in the passwd file (as cleartext) together with the hash of the salted password.



/etc/shadow

← → ⌂ 🔒 안전함 | <https://www.cyberciti.biz/faq/understanding-etcshadow-file/>

Info on the Linux Kernel Meltdown/Spectre Vulnerability

Understanding /etc/shadow file

in BASH Shell, CentOS, Debian / Ubuntu, FreeBSD, HP-UX Unix, Linux, RedHat and Friends, Solaris-Unix, Suse, Ubuntu Linux, UNIX, User Management

last updated August 2, 2017

C an you explain /etc/shadow file format used under Linux or UNIX-like system?

The **/etc/shadow** file stores actual password in encrypted format (more like the hash of the password) for user's account with additional properties related to user password. Basically, it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in [/etc/passwd file](#). Generally, shadow file entry looks as follows (click to enlarge image):



/etc/shadow

shadow(5) - Linux man page

Name

shadow - shadowed password file

Description

shadow is a file which contains the password information for the system's accounts and optional aging information.

This file must not be readable by regular users if password security is to be maintained.

Each line of this file contains 9 fields, separated by colons (":"), in the following order:

login name

It must be a valid account name, which exist on the system.

encrypted password

Refer to [crypt\(3\)](#) for details on how this string is interpreted.

If the password field contains some string that is not a valid result of *, the user will not be able to use a unix password to log in (but the i by other means).

This field may be empty, in which case no passwords are required to specified login name. However, some applications which read the /etc not to permit any access at all if the password field is empty.

A password field which starts with a exclamation mark means that the remaining characters on the line represent the password field before

date of last password change

The date of the last password change, expressed as the number of days since Jan 1, 1970. The value 0 has a special meaning, which is that the user should change his/her password the first time she will log in the system.



An empty field means that password aging features are disabled.

/etc/shadow file fields

vivek:\$1\$Infffc\$pGteyHdicpGOfffXX4ow#5:13064:0:99999:7::
1 2 3 4 5 6

(Fig.01: /etc/shadow file fields)



1. **Username**: It is your login name.
2. **Password**: It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to \$id\$salt\$hashed, The \$id is the algorithm used On GNU/Linux as follows:
 1. \$1\$ is MD5
 2. \$2a\$ is Blowfish
 3. \$2y\$ is Blowfish
 4. \$5\$ is SHA-256
 5. \$6\$ is SHA-512
3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

DIY please

```
jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-  
0044,email:/home/jsmith:/bin/sh
```

The fields, in order from left to right, are:^[1]

1. User name: the string a user would type in when logging into the operating system: the [logname](#). Must be unique across users listed in the file.
2. Information used to validate a user's [password](#); in most modern uses, this field is usually set to "x" (or "*", or some other indicator) with the actual password information being stored in a separate [shadow password file](#). On [Linux](#) systems, setting this field to an asterisk ("*") is a common way to disable direct logins to an account while still preserving its name, while another possible value is "*NP*" which indicates to use an [NIS](#) server to obtain the password.^[2] Without password shadowing in effect, this field would typically contain a cryptographic hash of the user's password (in combination with a [salt](#)).
3. [user identifier](#) number, used by the operating system for internal purposes. It need not be unique.
4. [group identifier](#) number, which identifies the primary group of the user; all files that are created by this [user](#) may initially be accessible to this group.
5. [Gecos field](#), commentary that describes the person or account. Typically, this is a set of comma-separated values including the user's full name and contact details.
6. Path to the user's [home directory](#).
7. Program that is started every time the user logs into the system. For an interactive user, this is usually one of the system's [command line interpreters \(shells\)](#).

Shadow file [\[edit \]](#)



[/etc/shadow](#) is used to increase the security level of passwords by restricting all but highly privileged users' access to hashed password data. Typically, that data is kept in files owned by and accessible only by the [super user](#).

crypt and DES

← → ⌂ 안전함 | <https://linux.die.net/man/>

Linux man pages

If you know the name of the Linux command, function, or library, you can search for it here.

Google Custom Search Search

Sections

Man pages are grouped into sections. To see the full list, click on one of the sections below.

- Section 1 user commands ([introduction](#))
- Section 2 system calls ([introduction](#))
- Section 3 library functions ([introduction](#))
- Section 4 special files ([introduction](#))
- Section 5 file formats ([introduction](#))
- Section 6 games ([introduction](#))
- Section 7 conventions and miscellany ([introduction](#))
- Section 8 administration and privileged commands ([introduction](#))
- Section L math library functions
- Section N tcl functions

← → ⌂ 안전함 | <https://linux.die.net/man/3/crypt>

crypt(3) - Linux man page

Name

crypt, **crypt_r** - password and data encryption

Synopsis

```
#define _XOPEN_SOURCE      /* See feature\_test\_macros(7) */
#include <unistd.h>

char *crypt(const char *key, const char *salt);
```

```
#define _GNU_SOURCE        /* See feature\_test\_macros(7) */
#include <crypt.h>
```

```
char *crypt_r(const char *key, const char *salt,
              struct crypt_data *data);
```

Link with `-lcrypt`.

Description

crypt() is the password encryption function. It is based on the Data Encryption Standard algorithm with variations intended (among other things) to discourage use of hardware implementations of a key search.

key is a user's typed password.

salt is a two-character string chosen from the set [a-zA-Z0-9./]. This string is used to perturb the algorithm in one of 4096 different ways.

By taking the lowest 7 bits of each of the first eight characters of the *key*, a 56-bit key is obtained. This 56-bit key is used to encrypt repeatedly a constant string (usually a string consisting of all zeros). The returned value points to the encrypted password, a series of 13 printable ASCII characters (the first two characters represent the salt itself). The return value points to static data whose content is overwritten by each call.

Warning: The key space consists of 2^{56} equal 7.2×10^{16} possible values. Exhaustive searches of this key space are possible using massively parallel computers. Software, such as **crack**(1), is available which will search the portion of this key space that is generally used by humans for passwords. Hence, password selection should, at minimum, avoid common words and names. The use of a **passwd**(1) program that checks for crackable passwords during the selection process is recommended.

설성카드 DIRECTAUTO

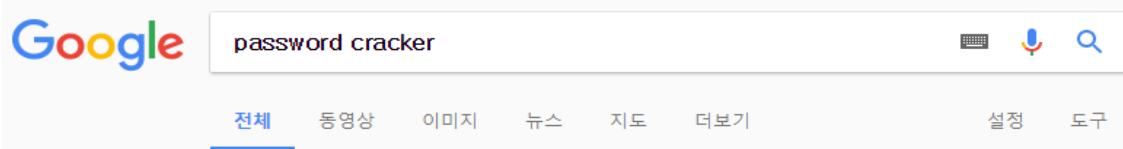
새 차를 사는 새로운 방법
다이렉트 오토!

60개월
3.2%

자세히보기



Password Crackers



Google search results for "password cracker". The search bar shows the query. Below it, a navigation bar includes tabs for 전체 (selected), 동영상, 이미지, 뉴스, 지도, 더보기, and buttons for 설정 and 도구. A search count of 904,000개 (0.58초) is displayed.

10 Most Popular Password Cracking Tools [Updated for 2017]
resources.infosecinstitute.com/10-popular-password-cracking-tools/ ▾ 이 페이지 번역하기
★★★★★ 평점: 5 - 작성자: By John Hollan" at GE
2017. 5. 25. - A password is the secret word or phrase that is used for the authentication process in various applications. It is used to gain access to accounts and resources. A password protects our accounts or resources from unauthorized access. What is Password Cracking? Password cracking is the process of ...
이 페이지를 2번 방문했습니다. 최근 방문 날짜: 18. 1. 7

10 Best Password Cracking Tools Of 2016 | Windows, Linux, OS X
<https://fossbytes.com/home/more/list/> ▾ 이 페이지 번역하기
2016. 7. 28. - Short Bytes: Password cracking is an integral part of digital forensics and pentesting. Keeping that in mind, we have prepared a list of the top 10 best password cracking tools that are widely used by ethical hackers and cybersecurity experts. These tools—including the likes of Aircrack, John the Ripper, and ...
이 페이지를 18. 1. 6에 방문했습니다.

Password Cracker - Free download and software reviews - CNET ...
download.cnet.com ▾ ... ▾ Security Software ▾ Encryption Software ▾ 이 페이지 번역하기
★★★★★ 평점: 1.4 - 리뷰 34개 - 무료 - Windows - 보안
Password Cracker by G&G Software is a tiny, free, totally portable utility that can recover lost passwords from applications. Passwords are perhaps the.

Password cracking - Wikipedia
https://en.wikipedia.org/wiki/Password_cracking ▾ 이 페이지 번역하기
In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the ...

Password Cracking Hacking Tools - Recommended Hacker Tools 2017
<https://www.concise-courses.com/hacking.../password-crackers/> ▾ 이 페이지 번역하기
2017. 9. 23. - Password hacking software has evolved tremendously over the last few years but essentially it comes down to several things: firstly, what systems are in place to prevent certain popular types of password cracking techniques (for example 'captcha forms' for brute force attacks), and secondly, what is the ...



Password Crackers

The screenshot shows a web browser window with the URL resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref. The page is titled "INFOSEC INSTITUTE". The main content discusses various password cracking tools, specifically mentioning Brutus and RainbowCrack.

1. Brutus

Brutus is one of the most popular remote online password cracking tools. It claims to be the fastest and most flexible password cracking tool. This tool is free and is only available for Windows systems. It was released back in October 2000.

It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. You can also create your own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resume and load options. So, you can pause the attack process any time and then resume whenever you want to resume.

This tool has not been updated for many years. Still, it can be useful for you.

2. RainbowCrack

RainbowCrack is a hash cracker tool that uses a large-scale time-memory trade off process for faster password cracking than traditional brute force tools. Time-memory trade off is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password much faster than brute force tools.

You also do not need to generate rainbow tables by yourselves. Developers of RainbowCrack have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. Like RainbowCrack, these tables are also available for free. You can download these tables and use for your password cracking processes.

Download Rainbow tables here: <http://project-rainbowcrack.com/table.htm>

- § Brutus
- § RainbowCrack
- § Wfuzz
- § Cain and Abel
- § John the Ripper
- § THC Hydra
- § Medusa
- § OphCrack
- § L0phtCrack
- § Aircrack-NG



Typical Password Rules

- § Trade-offs among enhanced security vs ability to remember
 - Site-specific rules add confusion

Password Rules

Certain rules should be followed to ensure that the password that you choose is secure:

1. Don't use names, surnames, pet names of family members, friends or pets, birthdays, anniversaries, or common phrases.
2. Spaces are not allowed at the beginning and end of passwords.
3. We impose the following password rules:
 - Your password has to be at least 6 characters long.
 - Must contain at least one lower case letter,
 - one upper case letter,
 - one digit
 - and one of these special characters ~!@#\$%^&*()_+
 - Your password will expire from time to time.
4. The best place to store your password is in your head, but if you tend to forget these types of things please make sure that you write your password down and store in a very secure place.



Typical Password Rules

- § Trade-offs among enhanced security vs ability to remember
- § Site-specific rules add confusion

안전하지 않음 | www.passwordmeter.com

Test Your Password		Minimum Requirements			
Password:	<input type="text"/>				
Hide:	<input checked="" type="checkbox"/>				
Score:	0%				
Complexity:	Too Short				
Additions		Type	Rate	Count	Bonus
✗ Number of Characters	Flat	$+(n*4)$	0	0	0
✗ Uppercase Letters	Cond/Incr	$+((len-n)*2)$	0	0	0
✗ Lowercase Letters	Cond/Incr	$+((len-n)*2)$	0	0	0
✗ Numbers	Cond	$+(n*4)$	0	0	0
✗ Symbols	Flat	$+(n*6)$	0	0	0
✗ Middle Numbers or Symbols	Flat	$+(n*2)$	0	0	0
✗ Requirements	Flat	$+(n*2)$	0	0	0
Deductions					
✓ Letters Only	Flat	$-n$	0	0	0
✓ Numbers Only	Flat	$-n$	0	0	0
✓ Repeat Characters (Case Insensitive)	Comp	-	0	0	0
✓ Consecutive Uppercase Letters	Flat	$-(n*2)$	0	0	0
✓ Consecutive Lowercase Letters	Flat	$-(n*2)$	0	0	0
✗ Consecutive Symbols	Flat	$-(n*2)$	0	0	0



RealMe, New Zealand Government

← → 🔒 Department of Internal Affairs [NZ] | <https://www2.logon.realme.govt.nz/cls/register/createmsllogon/createmsllogon?cid=2>

Password

Your password must be at least 7 characters long. If it is less than 12 characters it must contain at least three of the below:

- uppercase (A-Z)
- lowercase (a-z)
- numbers (0-9)
- symbols (e.g. #, \$, !, @, ^, &, *, etc)

Security questions

If you need to reset your password, you'll have to answer your security questions to access your login.

Question 1

Choose question 1

Choose question 1

What road did your best friend in secondary/high school live on?
What is the middle name of your oldest child?
What was the first name of your first girlfriend or boyfriend?
What was the name of the first company you worked for?
What is your grandmother's first name on your father's side?
What was the primary school you attended the most?
What is your oldest cousin's first name?
What is the name of the suburb you first grew up in?

Question 3

Choose question 3

Answer 3

Secret PIN (Optional)

If you want to add a secret PIN it will need to:

- be a five digit number
- have no more than three consecutive numbers
- not repeat the same digit more than twice





WHAT IT IS PRIVACY & SECURITY FOR BUSINESS HELP ABOUT SEARCH

NEWS >

This afternoon we have been alerted to a phishing email scam that is being targeted toward New Zealanders

7 Mar 2018

This afternoon we have been alerted to a phishing email scam that is being targeted toward New Zealanders. People have received an email stating that the user has a private message and they need to access their RealMe account. The web link in the email then takes the user to a fake RealMe website that requests the user to validate their identity and upload personal documents (passport and driver's license).

If you receive this RealMe phishing email do not click the web link. Please report the email to:
<https://www.cert.govt.nz/businesses-and-individuals/report-an-issue/>

These emails are coming from non-government email addresses and direct users to non-government web sites.

Neither the RealMe website itself or any customer accounts have been hacked or compromised.

Phishing attacks use 'spoof' emails and fraudulent websites designed to entice recipients into divulging personal financial data such as credit card numbers, identity details, bank and other account usernames and passwords.



← → C | 안전한 | https://www.google.com/search?newwindow=1&biw=1102&bih=1062&tbo=isch&sa=1&ei=8CYOW7OxHYqx8QWrhbroAQ&q=treat+your+password+like+your+... 🔍 ☆ 🔍 🔍

Google

treat your password like your |

treat your password like your underwear
treat your password like your toothbrush
treat your password like your underpants

Remove Report inappropriate predictions

View saved SafeSearch ▾

smegma secure hacked instagram account incorrect yout underwear delicately pulau pangkor scott heath

THINK SECURE

TREAT YOUR PASSWORDS LIKE YOUR UNDERWEAR

- CHANGE THEM OFTEN
- DON'T LEAVE THEM LYING AROUND
- DON'T SHARE THEM

Use strong pin for passwords. Keep them personal and save. Use different passwords for business and personal purposes.

THE COMPARED PERCEPTIONS OF PASSWORDS AND UNDERWEAR
Web Survey for Hustle / October 2015

1) THE RELATIVE QUANTITIES
Would you say that you have more pairs of underwear (panties, shorts) or passwords?

Countries	Percentage
France	83%
Germany	83%
Spain	79%
UK	76%
Italy	73%
Netherlands	70%
Australia	67%
USA	63%
Canada	60%
Japan	58%
China	55%

PASSWORDS ARE LIKE UNDERWEAR

You shouldn't leave them out where people can see them. You should change them regularly. And you shouldn't loan them out to strangers.

2) PASSWORDS VS PANTIES
Speaking about your underwear and your passwords, how often do you change them?

SECURITY CAT WANTS YOU TO TREAT YOUR PASSWORDS LIKE YOUR UNDERWEAR

Change them often! Keep them off your desk! Never share them with anyone!

3) SHARING OF PASSWORDS / UNDERWEAR WITH CLOSE RELATIVES
Have you ever shared your underwear or password with a friend or a member of your family?

THINK SECURE

Treat your passwords like your underwear

- Change them often
- Don't share with anyone
- Don't leave them lying around

Passwords are like underwear

Passwords are like underwear... Change yours often!
Passwords are like underwear... Don't share them with friends!
Passwords are like underwear... The longer, the better!
Passwords are like underwear... Don't leave yours lying around!

TREAT YOUR PASSWORDS LIKE YOUR UNDERPANTS

Change them often. Don't leave them lying around. And most importantly, don't share them.

Tips to create strong passwords

- Use different passwords everywhere
- Treat your passwords like your underwear
- Always common words and numbers
- Insert capital letters in unusual places
- Use a simple password but move your fingers on the keyboard one place to the left or right
- Longer passwords are harder to crack
- Substitute numbers for letters
- Think of a phrase you can remember and use the first letters of each word in the phrase
- Add special characters

← → C 안전한 | https://www.google.com/search?newwindow=1&biw=1102&bih=1062&tbo=isch&sa=1&ei=EicOW8fyN4iY8QWzha-4CA&q=treat+your+password+like+your+to... 🔍 ☆ ✎

Google

treat your password like your

treat your password like your underwear
treat your password like your toothbrush
treat your password like your underpants

Remove Remove

View saved SafeSearch ▾

cartoon cyber clifford stoll computer safety anybody else quotes Report inappropriate predictions posters

TREAT YOUR PASSWORD LIKE YOUR TOOTHBRUSH
keepitsafe.auburn.edu

TREAT YOUR PASSWORD LIKE YOUR TOOTHBRUSH
© 2014 THE SECURITY AWARENESS COMPANY

Treat your password like your toothbrush.
Don't let anybody else use it,
and get a new one every six months.
~ Clifford Stoll

Treat your password like your toothbrush.
Don't let anybody else use it,
and get a new one every six months.

Treat your Password LIKE Your Toothbrush
Never share it and change it often!

eSafety health check

STAY SAFE ONLINE

Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.

Clifford Stoll

lolsottrue:#448

A password is like a toothbrush

Choose a good one
Don't share it with anyone
Change it occasionally

PASSWORDS ARE LIKE UNDERWEAR

THE MOST COMMON PASSWORDS OF 2011 WERE:

PASSWORD 123456 12345678 QWERTY ABC123
MONKEY 1234567 LETMEIN TRUSTN01 DRAGON
BASBALL 111111 LOVEMYMASTER SUNSHINE
ASHLEY BAILEY PASSWORD SHADOW 123123
eH4LL SUPREME G4Z0WX MICHAEL FOOTBALL
**TREAT YOUR PASSWORD LIKE A TOOTHBRUSH:
CHOOSE A GOOD ONE, CHANGE IT EVERY 3 MONTHS & DON'T SHARE IT.**

How Password Crackers Work

- § Build a large dictionary of possible passwords and try each of these against the password file
 - Each password must be hashed using each salt value in the password file and then compared to stored hash values
 - Password cracking program may attempt variations (e.g., backward spelling, additional numbers or special characters, etc) on all the words in its dictionary of likely passwords
 - Requires huge computational overhead



Rainbow Table

- § Or, potential hash values can be precomputed
- § Attacker generates a large dictionary of possible passwords. For each password, the attacker generates the hash values associated with each possible salt value
 - Rainbow Table
 - 1.4GB data, cracking 99.9% of all alphanumeric Windows password hashes in 13.8 secs [Oechslin, Crypto, 2003]
- § Larger salt values and a sufficiently large hash values can make such attacks less practical
- § Rainbow tables and/or password crackers are readily available (free or for fee)



IMAP, NNTP, NetBus, etc. You can also create your own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resume and load options. So, you can pause the attack process any time and then resume whenever you want to resume.

This tool has not been updated for many years. Still, it can be useful for you.

2. RainbowCrack

RainbowCrack is a hash cracker tool that uses a large-scale time-memory trade off process for faster password cracking than traditional brute force tools. Time-memory trade off is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password much faster than brute force tools.

You also do not need to generate rainbow tables by yourselves. Developers of RainbowCrack have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. Like RainbowCrack, these tables are also available for free. You can download these tables and use for your password cracking processes.

Download Rainbow tables here: <http://project-rainbowcrack.com/table.htm>

A few paid rainbow tables are also available, which you can buy from here: <http://project-rainbowcrack.com/buy.php>

This tool is available for both Windows and Linux systems.

Download Rainbow crack here: <http://project-rainbowcrack.com/>

3. Wfuzz

Wfuzz is another web application password cracking tool that tries to crack passwords with brute forcing. It can also be used to find hidden resources like directories, servlets and scripts. This tool can also identify different kind of injections including SQL Injection, XSS Injection, LDAP Injection, etc in Web applications.



The screenshot shows a web browser window with the URL 'project-rainbowcrack.com/table.htm'. The page has a dark header with the 'RainbowCrack' logo and navigation links for Home, Documentation, Rainbow Tables, Performance, Buy Rainbow Tables, and Contact. Below the header is a large section titled 'List of Rainbow Tables'.

List of Rainbow Tables

This page lists the rainbow tables we generated.

LM rainbow tables speed up cracking of password hashes from Windows 2000 and Windows XP operating system.

NTLM rainbow tables speed up cracking of password hashes from Windows Vista and Windows 7 operating system.

MD5 and SHA1 rainbow tables speed up cracking of MD5 and SHA1 hashes, respectively.

The largest rainbow tables here are ntlm_mixalpha-numeric#1-9, md5_mixalpha-numeric#1-9 and sha1_mixalpha-numeric#1-9. Each has a key space of 13,759,005,997,841,642 (i.e., $2^{53.6}$).

Benchmark result of each rainbow table is shown in last column of the list below. We generate hashes of random plaintexts and crack them with the rainbow table and rcrack/rcrack_cuda/rcrack_cl program. rcrack program uses CPU for computation and rcrack_cuda/rcrack_cl program uses NVIDIA/AMD GPU.

Video demonstration of some rainbow tables on [YouTube](#):

- Hash Cracking with Rainbow Table ntlm_ascii-32-95#1-8
- Hash Cracking with Rainbow Table md5_ascii-32-95#1-8
- Hash Cracking with Rainbow Table sha1_ascii-32-95#1-8

Perfect rainbow tables are rainbow tables without identical end points, produced by removing merged rainbow chains in normal rainbow tables. To achieve same success rate, perfect rainbow tables are smaller and faster to lookup than non-perfect rainbow tables. In lists below, parameters of non-perfect rainbow tables are in gray.

Rainbow Tables

LM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
■ lm_ascii-32-65-123-4#1-7	ascii-32-65-123-4	1 to 7	7,555,858,447,479	99.9 %	27 GB 32 GB	Perfect Non-perfect	Perfect Non-perfect

NTLM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
■ ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
■ ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect



Password Selection Strategies

	How it works	Pros	Cons
User Education			
Computer-generated passwords			
Reactive password checking			
Proactive password checking			



Security Issues for User Authentication

Attacks	Authentication	Examples	Typical Defenses
Client Attack	Password		
	Token		
	Biometric		
Host Attack	Password		
	Token		
	Biometric		
Eavesdropping, theft, and copying	Password		
	Token		
	Biometric		
Replay	Password		
	Token		
	Biometric		
Trojan Horse	Password, token, biometric		
Denial of Service	Password, token, biometric		



Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of	Password, token,	Lockout by multiple	Multifactor with token

* Table 3.4,
Stallings and
Brown

Two factor authentication

§ DIY (Google, Facebook, Microsoft, Apple)

안전함 | <https://www.google.com/search?q=two+factor+authentication&rlz=1C1JZAI>

[Two-Factor Authentication: Who Has It and How to Set It Up | PCMag ...](https://www.pcmag.com/.../two-factor-authentication-who-has-it-and-how-to-set-it-up)

<https://www.pcmag.com/.../two-factor-authentication-who-has-it-and-how-to-set-it-up> ▾

1 day ago - What you really need is a second factor of authentication. That's why many internet services, a number of which have felt the pinch of being hacked, have embraced **two-factor authentication** for their users. It's sometimes called 2FA, or used interchangeably with the terms "two-step" and "verification" ...

[Two-factor authentication: What you need to know \(FAQ\) - CNET](https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/)

<https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/> ▾

Jun 15, 2015 - Twitter's got it. Apple's got it, too. Google, Microsoft, Facebook and Amazon have had it for a while. But why's **two-factor authentication** important, and will it keep you safe?

People also ask

[Can I turn off two factor authentication?](#)

[What is two factor theory?](#)

[How does two factor authentication work?](#)

[What does two factor authentication mean?](#)

Top stories



Google: Less than 10% of Gmail users enable two-factor authentication

TechRepublic

3 hours ago



Most Gmail users ignore two-factor authentication, sacrificing security for convenience

Washington Times

21 hours ago



Most Google Accounts Don't Use Two-Factor Authentication

PCMag India

1 day ago

→ More for two factor authentication

[What is two-factor authentication \(2FA\)? - Definition from WhatIs.com](https://searchsecurity.techtarget.com/definition/two-factor-authentication-2fa)

<https://searchsecurity.techtarget.com/definition/two-factor-authentication-2fa> ▾

Dec 21, 2016 - **Two-factor authentication** (2FA) is a security process for user authentication through two methods, one of which is usually a password.

[Google 2-Step Verification](https://www.google.com/landing/2step/)

<https://www.google.com/landing/2step/> ▾

It's easier than you think for someone to steal your password. Any of these common actions could put you at risk of having your password stolen: Using the same password on more than one site; Downloading software from the Internet; Clicking on links in email messages. 2-Step Verification can help keep bad guys out, ...

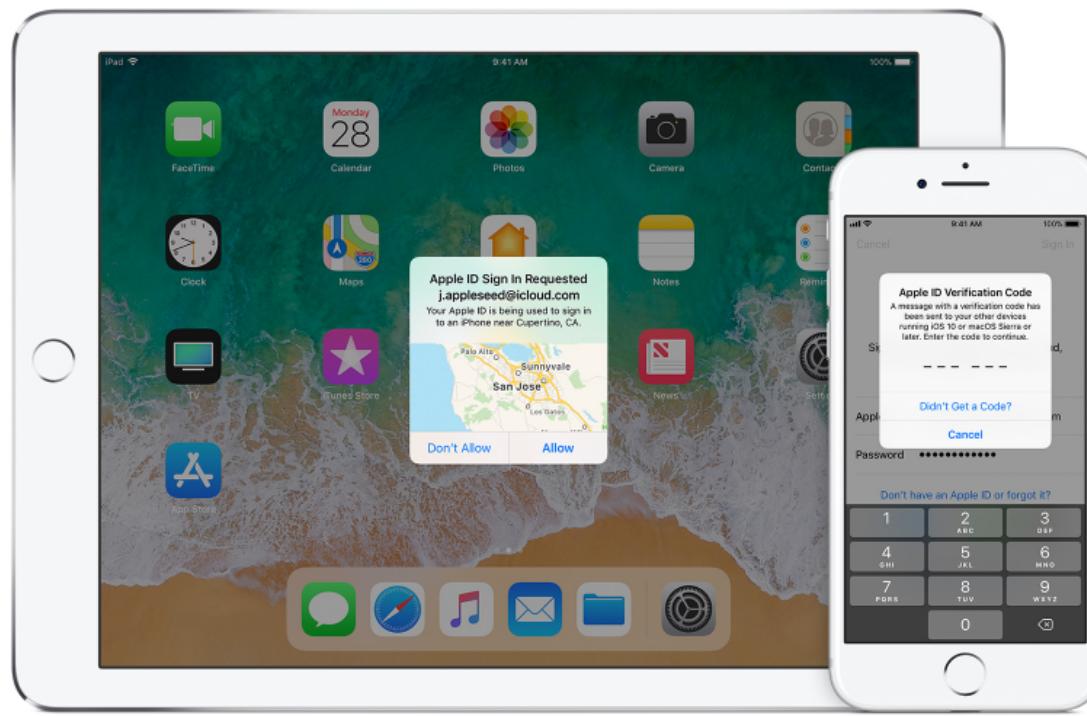


Apple Two Factor Authentication

A screenshot of a web browser displaying the Apple Support website at <https://support.apple.com/en-us/HT204915>. The page title is "Two-factor authentication for Apple ID". The navigation bar includes links for Mac, iPad, iPhone, Watch, TV, Music, and Support. The main content area describes two-factor authentication as an extra layer of security for your Apple ID.

Two-factor authentication for Apple ID

Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password.



How it works

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information—your password and the six-digit verification code that's automatically displayed on your trusted devices. By entering the code, you're verifying that you trust the new device. For example, if you have an iPhone and are signing into your account for the first time on a newly purchased Mac, you'll be prompted to enter your password and the verification code that's automatically displayed on your iPhone.

Because your password alone is no longer enough to access your account, two-factor authentication dramatically improves the security of your Apple ID and all the personal information you store with Apple.

Once signed in, you won't be asked for a verification code on that device again unless you sign out completely, erase the device, or need to change your password for security reasons. When you sign in on the web, you can choose to trust your browser, so you won't be asked for a verification code the next time you sign in from that computer.

Trusted devices

A trusted device is an iPhone, iPad, or iPod touch with iOS 9 and later, or a Mac with OS X El Capitan and later that you've already signed in to using two-factor authentication. It's a device we know is yours and that can be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser.

Trusted phone numbers

A trusted phone number is a number that can be used to receive verification codes by text message or automated phone call. You must verify at least one trusted phone number to enroll in two-factor authentication.

You should also consider verifying other phone numbers you can access, such as a home phone, or a number used by a family member or close friend. You can use these numbers if you temporarily can't access your own devices.



As you might have feared ...

Google attacks on apple two factor authentication

All News Videos Images More Settings Tools

About 1,160,000 results (0.52 seconds)

Five Most Common Security Attacks on Two-Factor Authentication
[https://www.itbusinessedge.com/.../five-most-common-security-attacks-on-two-factor-... ▾](https://www.itbusinessedge.com/.../five-most-common-security-attacks-on-two-factor-...)
Following some high-profile password hacks, companies like Apple, Twitter and Evernote have moved to shore up their systems with **two-factor authentication**. Said to be a great missing security link in many password-driven systems, **two-factor authentication** technologies that are most widely used today are actually fraught ...

People also search for

how to bypass 2 factor authentication is 2 step verification worth it
access control attacks hybrid password attack
authentication vulnerabilities authenticated and unauthenticated attacks

Apple to auto-update devices to two-factor authentication – Naked ...
[https://nakedsecurity.sophos.com/.../apple-to-auto-update-devices-to-two-factor-authe... ▾](https://nakedsecurity.sophos.com/.../apple-to-auto-update-devices-to-two-factor-authe...)
.Jun 12, 2017 - Has Apple really mandated the use of **two-factor authentication** (2FA) for beta users of macOS High Sierra iOS 11? And would ... This design is vulnerable to man-in-the-middle **attacks** and SIM-swap frauds, which is why Apple wants to shunt users on to its **two-factor authentication** if it can. In addition to ...

Two-Factor Authentication Bypassed in Simple Attacks | SecurityWeek ...
[https://www.securityweek.com/two-factor-authentication-bypassed-simple-attacks ▾](https://www.securityweek.com/two-factor-authentication-bypassed-simple-attacks)
Apr 12, 2016 - According to the researchers, their SMS stealing app was uploaded to Google Play on July 8, 2015, and was available in the store for **two** months, until they shared its name and a video demonstration of the **attack**, although the Android security team was informed months before the initial publication. Apple ...

This is why you shouldn't use texts for two-factor authentication - The ...
[https://www.theverge.com/.../9/.../sms-two-factor-authentication-hack-password-bitcoi... ▾](https://www.theverge.com/.../9/.../sms-two-factor-authentication-hack-password-bitcoi...)
Sep 18, 2017 - There are a few concrete steps you can take to protect yourself from this kind of **attack**. On some services, you can revoke the option for SMS **two-factor** and account recovery entirely, which you should do as soon as you've got a more secure app-based method established. Google, for instance, will let you ...

Hackers using phishing to bypass 2FA (two-factor authentication)
[https://www.wandera.com/blog/bypassing-2fa/ ▾](https://www.wandera.com/blog/bypassing-2fa/)
Jan 29, 2018 - However, like so many other security features, it is a mistake to assume this defense against **attack** is watertight. A 2FA-protected account is still vulnerable to **attack**, even among the most widely used and trusted services. That includes enterprise services like Apple, Microsoft, Paypal and LinkedIn. So how ...





two factor authentication google



All

Images

Videos

News

Maps

More

Settings

Tools

About 4,080,000 results (0.70 seconds)

Google 2-Step Verification

<https://www.google.com/landing/2step/> ▾

It's easier than you think for someone to steal your password. Any of these common actions could put you at risk of having your password stolen: Using the same password on more than one site; Downloading software from the Internet; Clicking on links in email messages. **2-Step Verification** can help keep bad guys out, ...

People also search for

X

gmail 2 step verification lost phone uplay google authenticator
google authenticator new phone two step verification apple
verify gmail account with phone number gmail verification code password recovery

Turn on 2-Step Verification - Google Account Help - Google Support

<https://support.google.com> › ... › Desktop web › Google Help for 2-Step Verification ▾

When you enable **2-Step Verification** (also known as **two-factor authentication**), you add an extra layer of security to your account. You sign in with something you know (your password) and something you.

People also ask

What is a two factor authentication? ▾

What is two factor authentication for Gmail? ▾

How do I get a barcode for Google Authenticator? ▾

How do you turn off two factor authentication on iPhone? ▾



OTP (One Time Password)

https://en.wikipedia.org/wiki/One-time_password



thus reducing the [attack surface](#) further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore, they require additional technology to work.

Contents [hide]

- 1 How OTPs are generated and distributed
- 2 Methods of generating the OTP
 - 2.1 Time-synchronized
 - 2.2 Mathematical algorithms
- 3 Methods of delivering the OTP
 - 3.1 Phones
 - 3.2 Proprietary tokens
 - 3.3 Web-based methods
 - 3.4 Hardcopy
- 4 Comparison of technologies
 - 4.1 Comparison of OTP implementations
 - 4.2 OTPs versus other methods of securing data
 - 4.3 Related technologies
- 5 Standardization
- 6 See also
- 7 References



Other Approaches to Authentication

§ Graphical Passwords

§ CAPTCHA

- My recent talk at a conference (KOCSEA Technical Symposium, Nov 2017, Univ of Nevada, Las Vegas)

§ ...



Graphical passwords

graphical password authentication paper

All Images Videos News More Settings Tools

About 446,000 results (0.94 seconds)

[PDF] Secure User Authentication & Graphical Password using Cued Click ...
https://arxiv.org/pdf/1505.01594.pdf
by SB Sahu - 2015 - Cited by 3 - Related articles
password mostly complicated to user take in mind. User authenticate password using cued click points and Persuasive Cued Click. Points graphical password scheme which includes usability and security evaluations. This paper includes the persuasion to secure user authentication & graphical password using cued ...

Graphical Password-Based ...
ieeexplore.ieee.org/document/7580200/
by M Martinez-Diaz - 2016 - Cited by 1 - Related articles
Dec 22, 2015 - Abstract: User authentication is a critical component of any system that deals with sensitive information. In this work, authentication is based on graphical password technology. The proposed scheme uses dynamic time warping and Gaussian mixture models for face verification ...

User authentication by ...
ieeexplore.ieee.org/document/4633110/
by SK Bandyopadhyay - 2008 - Cited by 1 - Related articles
There are numerous Biometric authentication schemes available. However, they are not always reliable. There is a need for a novel and new alternative. Figure shows a graphical password scheme where users can select their Passwords. In this paper we propose a graphical password scheme based on ...

Alignment based graphical ...
ieeexplore.ieee.org/document/7580200/
by A Danish - 2016 - Cited by 2 - Related articles
Oct 31, 2016 - Abstract: Previous research has shown that graphical passwords are more memorable than alphanumeric username and password schemes. However, graphical password i.e. it provides better security and convenience as compared to alphanumeric password because it is easier to remember so they ...

www.realuser.com

passfaces™

Graphical Password Technology

Home About Products Try Passfaces Support Resources News Partners Contact Us Portal Logon

Passfaces: Two Factor Authentication for the Enterprise

Passfaces are graphical passwords that use faces as a unique verification technology for secure logon. Offering two factor authentication to provide a high level of authentication assurance, Passfaces supports a wide range of operating environments in which strong authentication is required. Passfaces Web Access easily integrates with existing security systems in financial, government, healthcare, and corporate networks. Passfaces is completely intuitive to use and combines two way authentication – user-to-site and site-to-user – in a single, reliable process.

What is Two Factor Authentication?

High Security

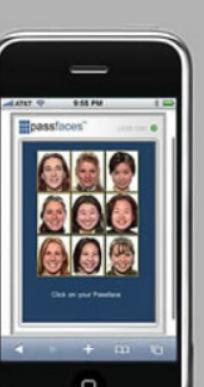
- Two factor = strong authentication
- Two way = mutual authentication
- Cognometric = personal authentication

User Convenience

- No tokens to lose or forget
- Fully mobile: use on any PC, iPhone etc.
- Completely intuitive: works every time

Low Cost

- Uses existing password infrastructure
- No new servers or databases
- Deploys in days – not weeks



click here to Try the Passfaces demo

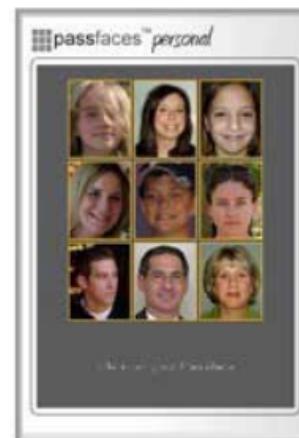
Experience Passfaces' unique, intuitive operation for yourself. Based on the innate human ability to recognize familiar faces, Passfaces works for all users – independent of age, language, education or culture.

KOREA UNIVERSITY





1st To setup, select from 1 to 5 faces from your collection of photos to use as your secret "Passfaces"



2nd To Logon, pick each of your Passfaces from groups containing 8 strangers

[Download Passfaces Personal Now](#)

NEW: Personalize Your Logon Experience with Passfaces Personal's Advanced Features

Create Entire Passfaces Logon Grids with Your Own Pictures

Create complete personalized Passfaces logon grids. Use pictures from your own PC, your Facebook* contacts, Web based photo library, or use photos of movie stars, sports heroes etc. from any Web site.

Make Logon Fun!



***Facebook - use your friend's pictures as your passfaces**

We've built a small Facebook application to help you choose your friend's pictures. Try it now: <http://apps.facebook.com/passfaces>



Share Your Passfaces Grids with Your Friends

Your personalized Passfaces grids can be shared with friends via email, IM or Facebook etc.

Choose Your Level of Security

Set from one to five secret Passfaces.



Diverse Approaches to Graphical Passwords

word by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

In Figure 1, we show an example of a user creating a graphical password. In this example, the user chooses a picture of his or her kids by pressing “Load Image button”. Then the user clicks on the kids faces in the order of their ages (order is enforced). For each selected region, the user types the kid’s name or nickname.



Figure 1. An example of creating a graphical password using the proposed system.



Figure 2. Login Screen

In the proposed system, a user freely chooses a picture, POIs and corresponding words. The order and number of POIs can be enforced for stronger authentication. Together, these parameters allow for a very large password space.

We believe that proposed approach is promising and unique for at least two reasons:

- It combines graphical and text-based passwords trying to achieve the best of both worlds.
- It provides multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system.



Other Approaches

Camera Based Two Factor Authentication Through Mobile and Wearable Devices

MOZHGAN AZIMPOURKIVI, Florida International University

UMUT TOPKARA, Bloomberg LP

BOGDAN CARBUNAR, Florida International University

Oct 2017

We introduce Pixie, a novel, camera based two factor authentication solution for mobile and wearable devices. A quick and familiar user action of snapping a photo is sufficient for Pixie to simultaneously perform a graphical password authentication and a physical token based auth based on both the knowledge a choose their trinkets similar to that the object is the trinket, i:

“Shoulder surfing” attack?

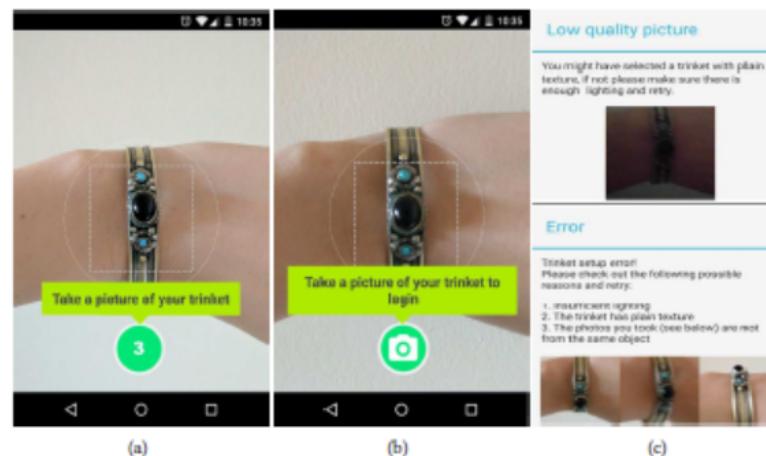


Fig. 1. Pixie: (a) Trinket setup. The user takes photos of the trinket placing it in the circle overlay. UI shows the number of photos left to take. (b) Login: the user snaps a photo of the trinket. (c) Trinket setup messages provide actionable guidance, when the image quality is low (top), or the reference images are inconsistent (bottom).



Yet Another Approach...

Sayli Chavan *et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 324-329

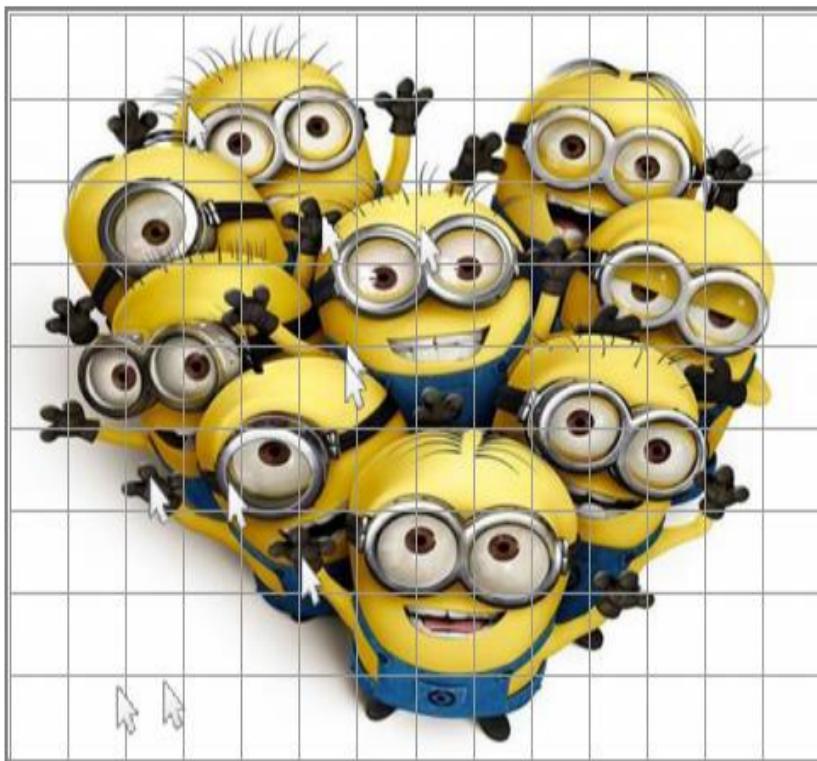


Fig.2: Grid Approach

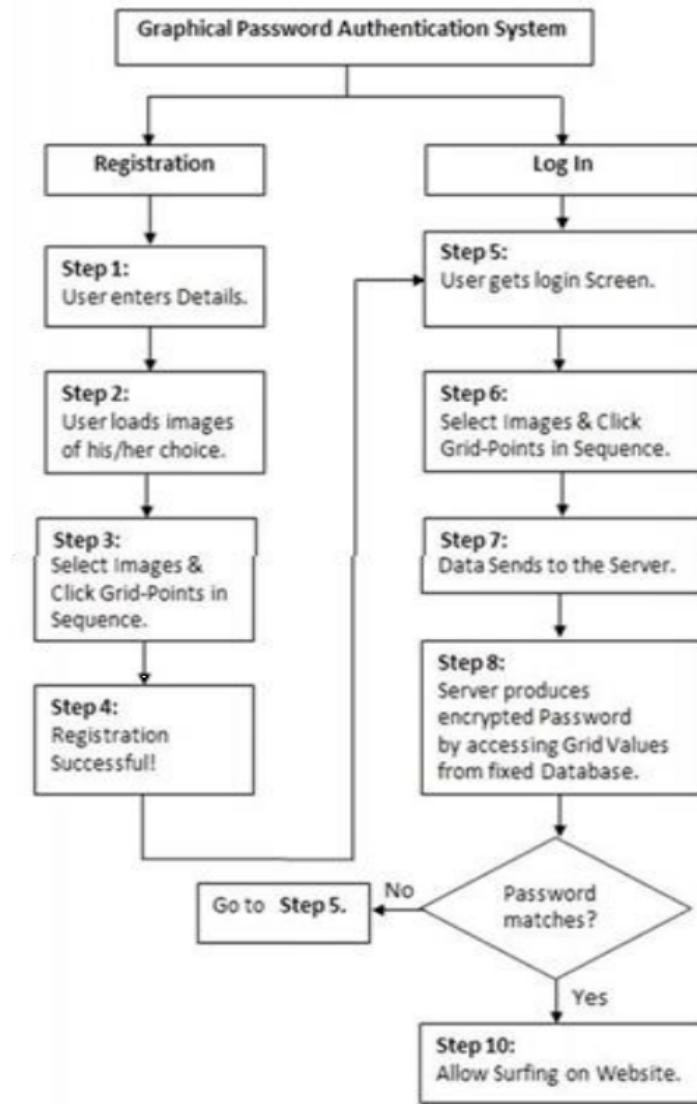


Fig.4: Flow graph.

CAPTCHA

- § Completely Automated Public Turing test to tell Computers and Humans Apart)
 - HIP (Human Interaction Proof)
- § Often complements text-based password
 - Strengthen security in user authentication
 - Reduce likelihood of service abuse (e.g., bogus account creation)
- § Widely used, but security enhancement might not be as substantial as expected



CAPTCHA

CAPTCHA

From Wikipedia, the free encyclopedia



This article **is written like a personal reflection or opinion essay** that states a Wikipedia editor's personal feelings about a topic. Please [help improve it](#) by rewriting it in an encyclopedic style. (January 2017) ([Learn how and when to remove this template message](#))

A **CAPTCHA** (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human.^[1]

The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford.^[2] The most common type of CAPTCHA was first invented in 1997 by two groups working in parallel: (1) Mark D. Lillibridge, Martin Abadi, Krishna Bharat, and Andrei Z. Broder; and (2) Eran Reshef, Gili Raanan and Eilon Solan.^[3] This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a [reverse Turing test](#).

This user identification procedure has received many criticisms, especially from disabled people, but also from other people who feel that their everyday work is slowed down by distorted words that are difficult to read. It takes the average person approximately 10 seconds to solve a typical CAPTCHA.^[citation needed]



This CAPTCHA of "smwm" obscures its message from computer interpretation by twisting the letters and adding slight background color gradient.

Contents [hide]

- 1 History
 - 1.1 Inventorship claims
- 2 Characteristics
- 3 Relation to AI
- 4 Accessibility
- 5 Circumvention
 - 5.1 Machine learning-based attacks
 - 5.2 Cheap or unwitting human labor
 - 5.3 Insecure implementation
 - 5.4 Notable attacks
- 6 Alternative CAPTCHAs schemas



- § What is your personal experience on CAPTCHA tests
- § How can CAPTCHA tests be defeated? Or, Can you?

W6 8HP



Security Check

Enter both words below, separated by a space.
Can't read the words above? Try different words or an audio CAPTCHA.

usual 18-MONTH

Text in the box:
usualmonth
What's this?

Submit **Cancel**



Type the two words:

CAPTCHA



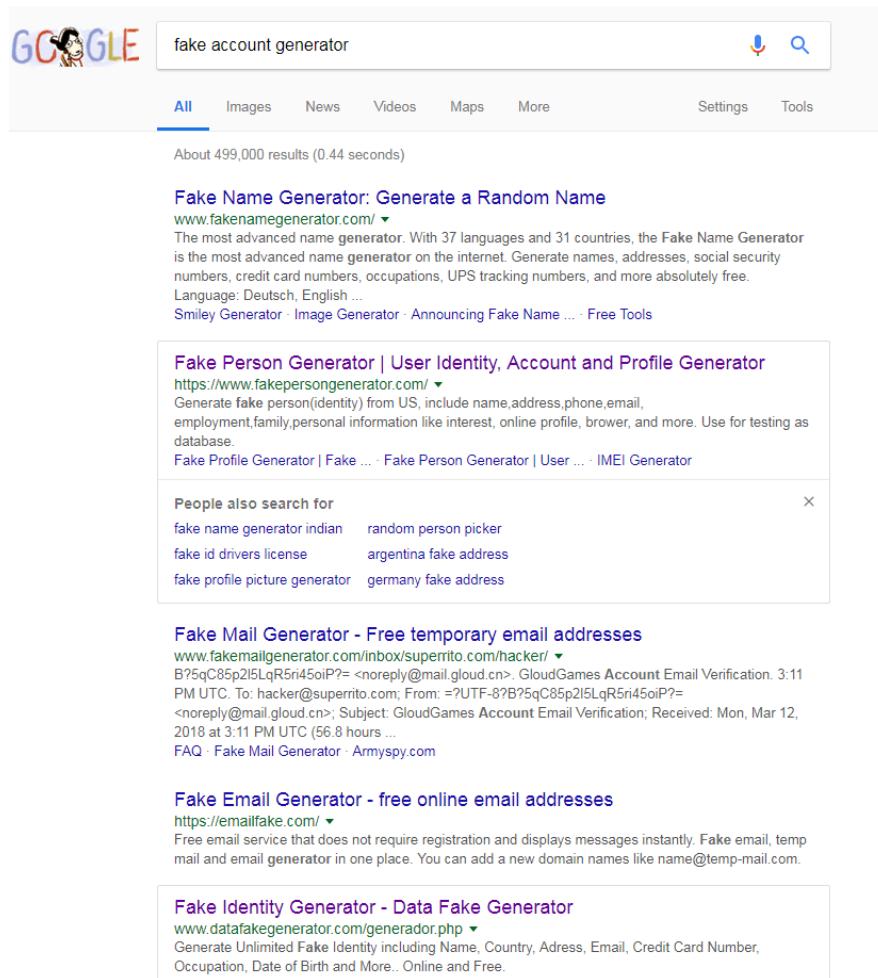
SXYBM SXYBM SXYBM
AWEVJ AWEVJ AWEVJ
KSYEM KSYEM KSYEM
EXHXC EXHXC EXHXC
BWARY BWARY BWARY
SKWH SKWH SKWH



CAPTCHA and “Bogus/Fake” Accounts

- § Sources of massive spam mails
- § What are possible impacts of having bogus accounts on

- Facebook
- Amazon
- Netflix...
- Google
- Microsoft
- ...



A screenshot of a Google search results page. The search query "fake account generator" is entered in the search bar. The results show several links related to generating fake names, profiles, and email addresses.

- Fake Name Generator: Generate a Random Name**
www.fakenamegenerator.com/ ▾
The most advanced name generator. With 37 languages and 31 countries, the Fake Name Generator is the most advanced name generator on the internet. Generate names, addresses, social security numbers, credit card numbers, occupations, UPS tracking numbers, and more absolutely free.
Language: Deutsch, English ...
Smiley Generator · Image Generator · Announcing Fake Name ... · Free Tools
- Fake Person Generator | User Identity, Account and Profile Generator**
<https://www.fakepersongenerator.com/> ▾
Generate fake person(identity) from US, include name,address,phone,email, employment,family,personal information like interest, online profile, brower, and more. Use for testing as database.
Fake Profile Generator | Fake ... · Fake Person Generator | User ... · IMEI Generator
- People also search for**
fake name generator indian random person picker
fake id drivers license argentina fake address
fake profile picture generator germany fake address
- Fake Mail Generator - Free temporary email addresses**
www.fakemailgenerator.com/inbox/superrito.com/hacker/ ▾
B?5qC85p2l5LqR5ri45oiP?= <noreply@mail.gloud.cn>. GloudGames Account Email Verification: 3:11 PM UTC. To: hacker@superrito.com; From: =>UTF-8?B?5qC85p2l5LqR5ri45oiP?= <noreply@mail.gloud.cn>; Subject: GloudGames Account Email Verification; Received: Mon, Mar 12, 2018 at 3:11 PM UTC (56.8 hours ...
FAQ · Fake Mail Generator · Armyspy.com
- Fake Email Generator - free online email addresses**
<https://emailfake.com/> ▾
Free email service that does not require registration and displays messages instantly. Fake email, temp mail and email generator in one place. You can add a new domain names like name@temp-mail.com.
- Fake Identity Generator - Data Fake Generator**
www.datafakegenerator.com/generador.php ▾
Generate Unlimited Fake Identity including Name, Country, Adress, Email, Credit Card Number, Occupation, Date of Birth and More.. Online and Free.



Identity Theft

§ Will not be discussed, but it is surely a real and serious threat

The screenshot shows a Google search results page for the query "identity theft". The search bar at the top contains the query. Below the search bar, there are tabs for "All", "Images", "News", "Videos", "Books", and "More". The "All" tab is selected. To the right of the tabs are "Settings" and "Tools" buttons. A user profile icon is in the top right corner.

About 75,100,000 results (0.63 seconds)

Identity Theft Recovery Steps | IdentityTheft.gov
https://www.identitytheft.gov/ ▾
Recovering from identity theft is a process. Here's step-by-step advice that can help you limit the damage, report identity theft, and fix your credit.
Warning Signs of Identity Theft · Log In · Federal Trade Commission · Sample Letters

People also ask

- Is identity theft a misdemeanor or a felony?
- Who do you call for identity theft?
- What do you do if your identity is stolen?
- How are victims affected by identity theft?

Feedback

Identity theft - Wikipedia
https://en.wikipedia.org/wiki/Identity_theft ▾
Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if ...
Techniques for obtaining ... · Indicators that you may be ... · Identity protection by ...

Identity Theft | Consumer Information
https://www.consumer.ftc.gov/features/feature-0014-identity-theft ▾
Identity theft tops the list of complaints to the FTC by consumers nationwide.

Identity Theft | USAGov
https://www.usa.gov/identity-theft ▾
Nov 6, 2017 - How to protect yourself against identity theft and respond if it happens.
Equifax Data Breach · Identity Theft · Prevent Identity Theft · Report Identity Theft



Identity theft

See Tfd Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. [Wikipedia](#)

People also search for [View 2+](#)

- Malware
- Spyware
- Trojan horse

Feedback



The .gov means it's official.
Federal government websites often end in .gov or .mil. Before sharing sensitive information, make sure you're on a federal government site.

This site is secure.
The https:// ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely.

USA.gov

Search All Government  Contact Us | 1-844-USA-GOV1

All Topics and Services  Government Agencies and Elected Officials  Benefits, Grants, Loans  Housing  Jobs and Unemployment  Money and Taxes  Travel and Immigration 

Español

Identity Theft

< Scams and Frauds

Common Scams and Frauds
Housing Scams
Identity Theft
Online Safety
Privacy
Report Scams and Frauds

How to protect yourself against identity theft and respond if it happens.

What's on This Page

- [Equifax Data Breach](#)
- [Prevent Identity Theft](#)
- [Tax ID Theft](#)
- [Identity Theft](#)
- [Report Identity Theft](#)
- [Medical ID Theft](#)

Equifax Data Breach

Equifax, one of the three major credit reporting agencies in the U.S., announced a data breach that affects 143 million consumers. The hackers accessed Social Security numbers, birthdates, addresses, and driver's license numbers.



Other Authentication Tools

- § Fingerprint
- § Retina
- § Face
- § ...
- § Will not be further discussed because we all use smartphones equipped with such authentication systems



Authentication challenges

- § NOT necessarily limited to passwords (e.g., mobile payment services, ...)
- § Remote user authentication is another challenge
- § Potential attacks include
 - client attack
 - host attack
 - eavesdropping, theft, and copying
 - replay
 - trojan horse
 - denial of service



Towards more robust authentication mechanism ("Adding uncertainty to improve user authentication")

Dr. Shinil Kwon, FormalWorks

Prof. Simon Woo, SUNY-Korea

Prof. Sungdeok (Steve) Cha, Korea University*

KOCSEA Technical Symposium
Nov 11th, 2017
UNLV, NV



Same old story...

Cyber-Safe

Google says hackers steal almost 250,000 web logins each week

by Selena Larson @selenalarson

Nov 9, 2017: 4:13 PM ET



CNN tech

All Control Panel Items > Windows Update

Windows Update

Download and install updates for your computer

8 important updates are available
5 optional updates are available

7 important updates selected, 304.7 MB
- 304.8 MB

Install updates

Most recent check for updates: Today at 14:34
Updates were installed: 07/06/2017 at 11:08. [View update history](#)
You receive updates: Managed by your system administrator

How to protect yourself from hackers



Tinder Gold is a massive hit



You'll soon be able to eat breakfast at Tiffany's first-ever cafe

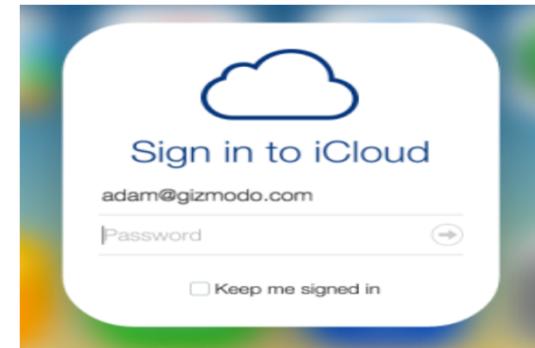


Uber partners with NASA ahead of flying taxi initiative



Google is digging into the dark corners of the web to better secure people's accounts.

Always Happening

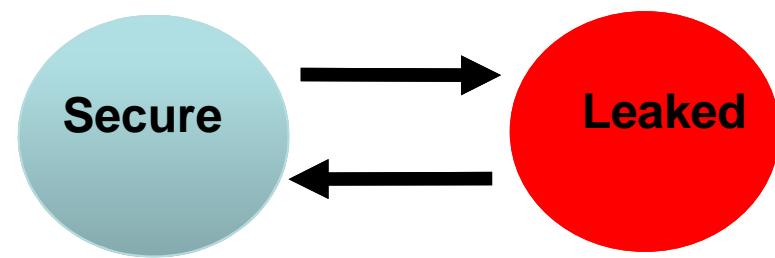


“Personal” Nightmare



§ This list is most likely the tip of the iceberg !

- Very (extremely?) difficult to remember
- Heavily reused, small candidate pools, special character rules, ...
- Difficult, if not impossible, to detect attacks in timely manner
- ...



Personal “trauma”?

한국연구재단 홈페이지에 오신것을 환영합니다.

로그인을 하시면 더 많은 서비스를 이용 하실 수 있습니다.

회원 로그인

[회원가입](#) | [아이디/비밀번호 찾기\(재단회원\)](#) | [아이디/비밀번호 찾기\(기관회원\)](#)

15

1. 본인확인서비스

4,8
2.6

D에 설명제를 시행하고 있습니다.

① 한국연구재단은 홈페이지서비스의 원활성을 기하고 서비스 이용과 홈페이지상에서의 익명 사용자로 인한 피해들을 방지하기 위해
② 아래의 인증방법 중 하나를 선택하여 본인확인을 해 주시기 바랍니다.



안심본인인증 본인확인

안심본인인증(대리인 가능)으로 본인확인

안심본인인증 서비스는 본인 명의 휴대폰, 개인용으로 유료 구입한 범용 공인인증서를 이용하여 온라인상에서 본인을 확인하는 서비스입니다.

안심본인인증 실패 관련 고객센터 : NICE평가정보 (☎ 1600-1522)

nice.checkplus.co.kr 내용:

고객님의 안전한 서비스 이용을 위하여
보안프로그램 설치가 필요합니다.
[확인]을 선택하시면 설치페이지로 연결됩니다.

확인

취소



New Authentication System using both Images and Texts

- § Create highly personalized association between image and text
 - § Image: easy to remember and upload
 - § Text: highly personalized

yummy
delicious

• • •

2014again!

• • • •

• • ? • • •

2017forever!



oh no 2017! • •



Proposed System: Account Creation / Login Session

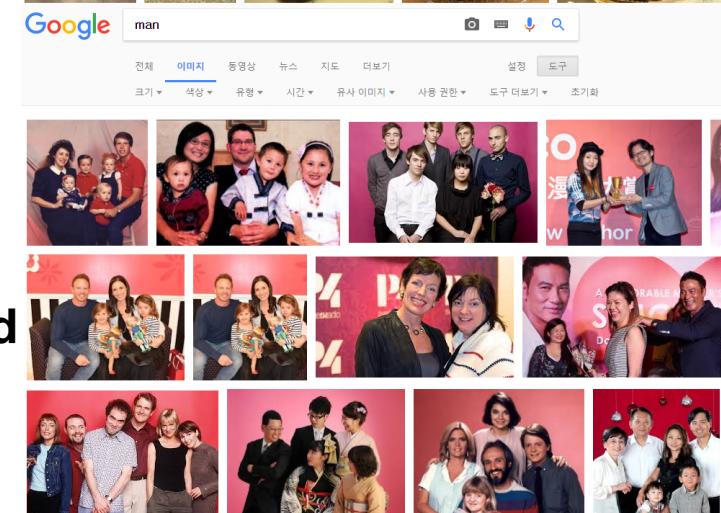
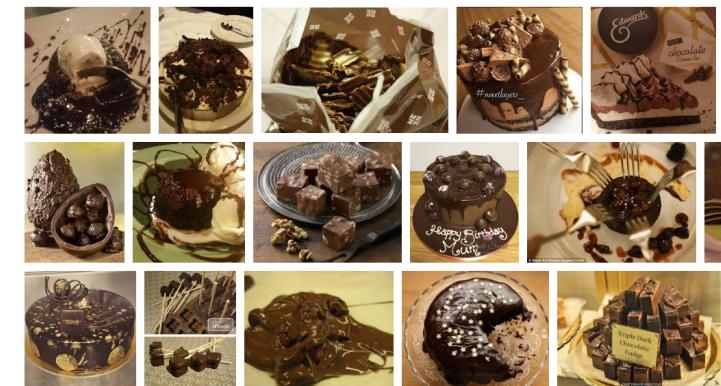
ID: sungdeok



user uploaded images &
short and highly personalized password

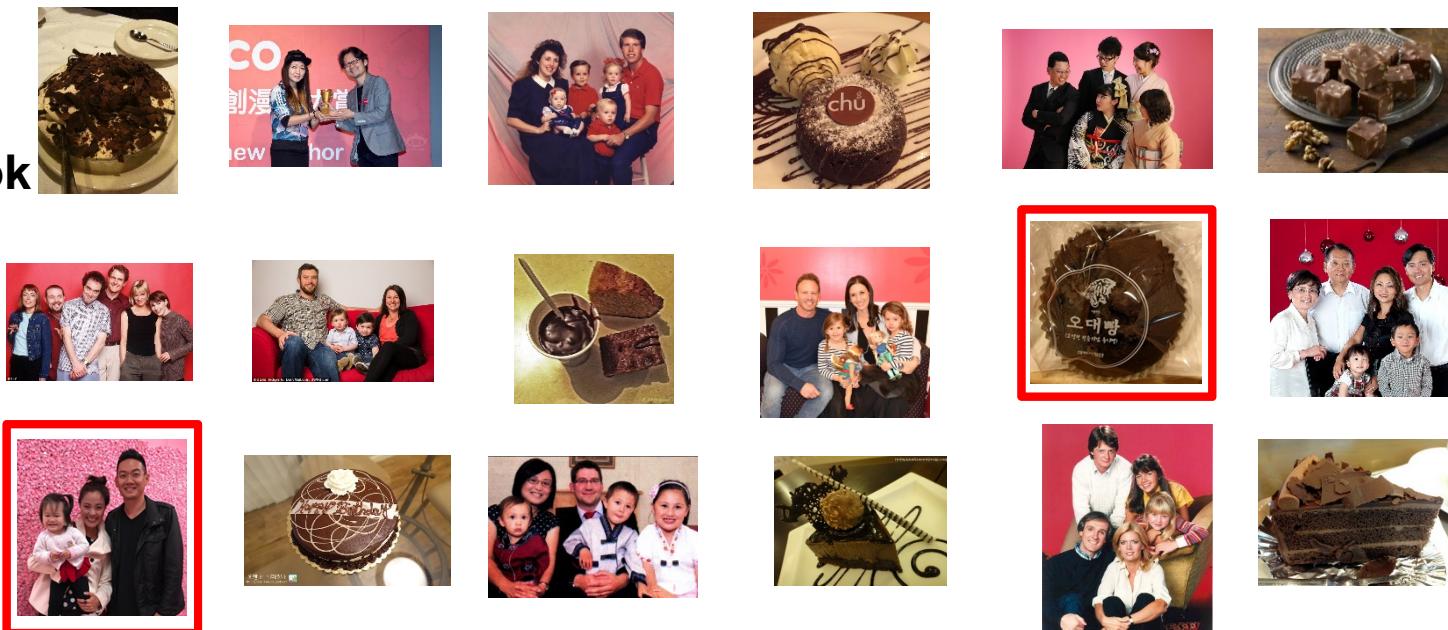


System generated “similar but different enough” images to the



Proposed System*: Password Verification

ID: sungdeok



oh no 2017! • •

Submit

In order to successfully authenticate:

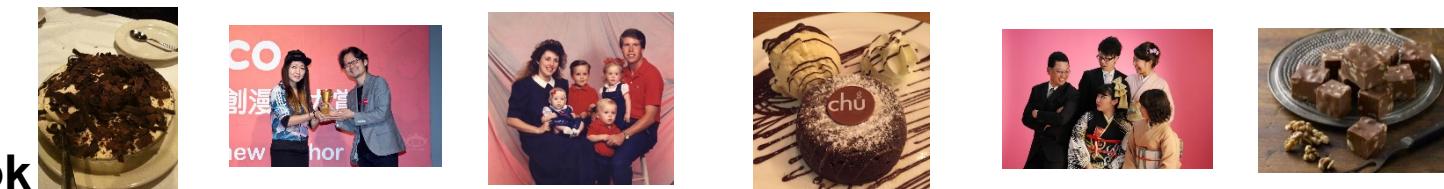
- ü Must correctly choose images
- ü Must provide the correct text associated with the images

* Not yet built



Another Possibility?

ID: sungdeok



eric• • •

Submit



Provided that the image in the lower right corner is NOT a “trap” image

Who Not?

ID: sungdeok



oh no 2017! • • , eric• • •

Submit



Provided that the image in the lower right corner is NOT a “trap” image

Actual deployment: TBD but should be flexible enough !

- § Same images? Different images?
- § Random placement of images?
- § Number of images presented vs to-be-clicked
 - Mobile vs PC
 - e.g., may allow selection of additional images if they are not “trap” images
- § How text password is entered
 - e.g., choose two images, but enter text associated with either image
 - To further introduce uncertainty while not confusing users
- § But, absolutely no feedback on failed login attempts !!!



Attack Scenario (1): Random (Human) Attacker

Password Verification

ID: sungdeok



celebration / happiness / oh happy day /

...

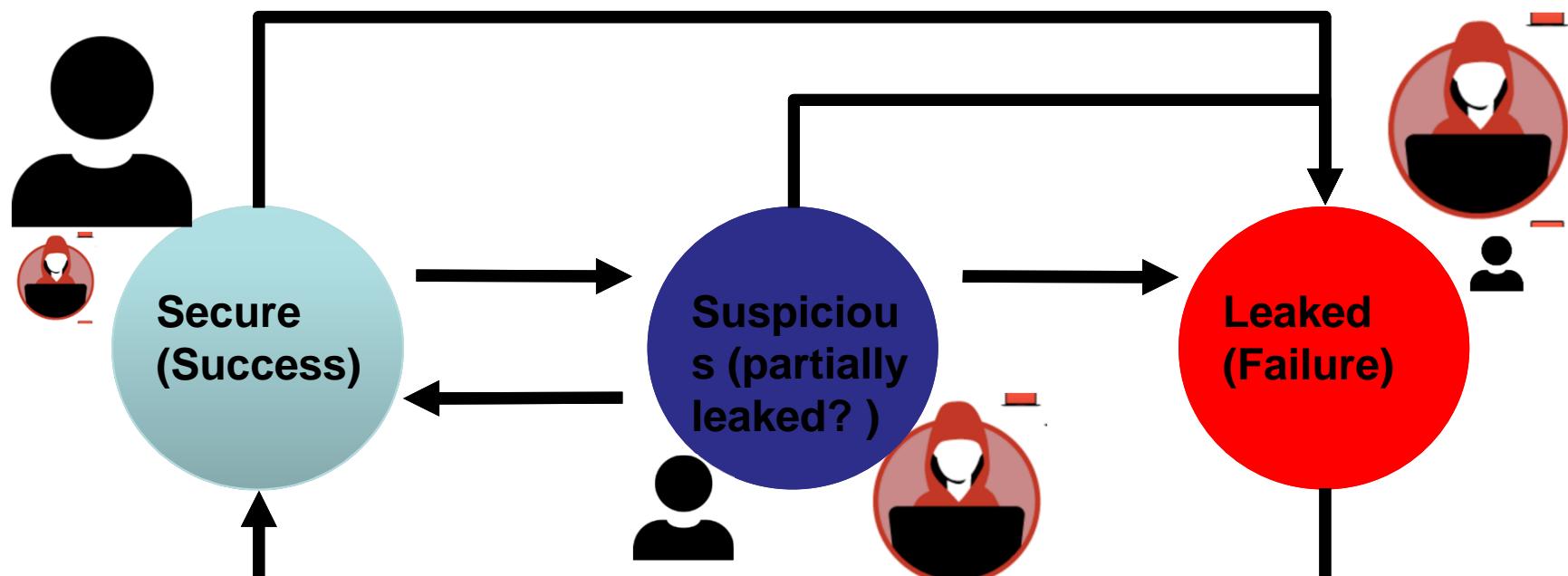
Submit



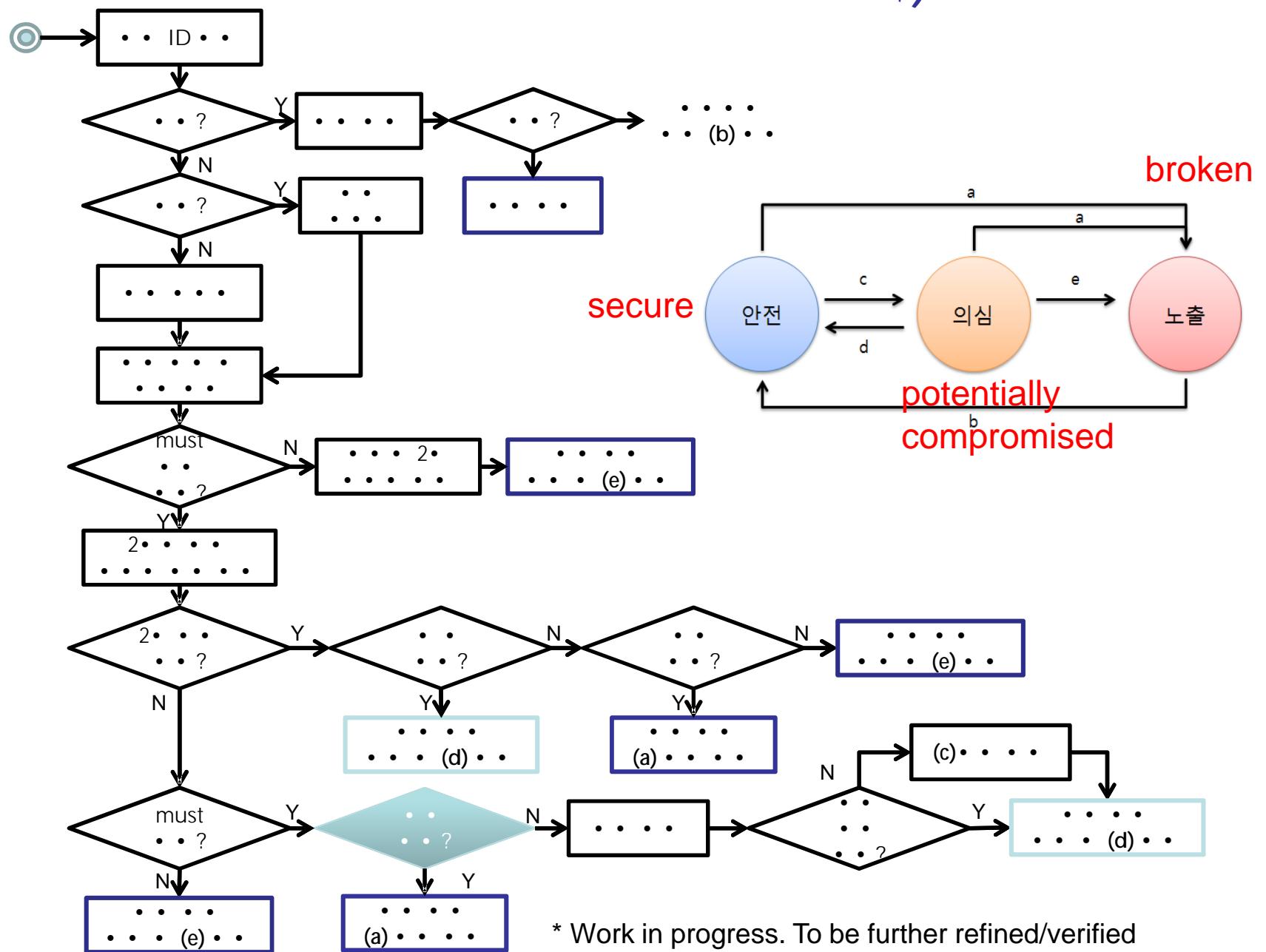
- Intruders are likely to choose wrong or trap images
- Intruders are highly unlikely to enter the correct text password
- Can it really survive “social engineering” attacks? To be explored.

Simplified User Authentication State

Based on user's image selection, and text responses, there are several different cases to consider



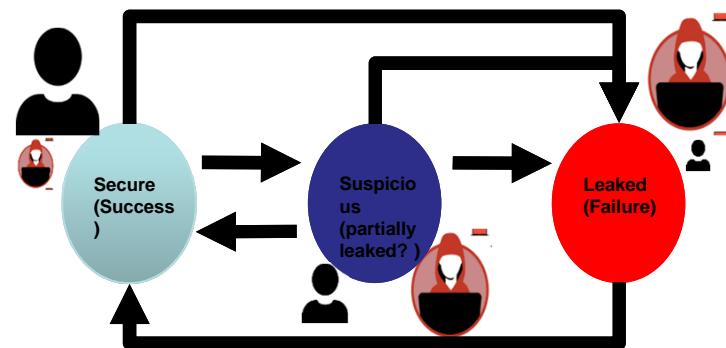
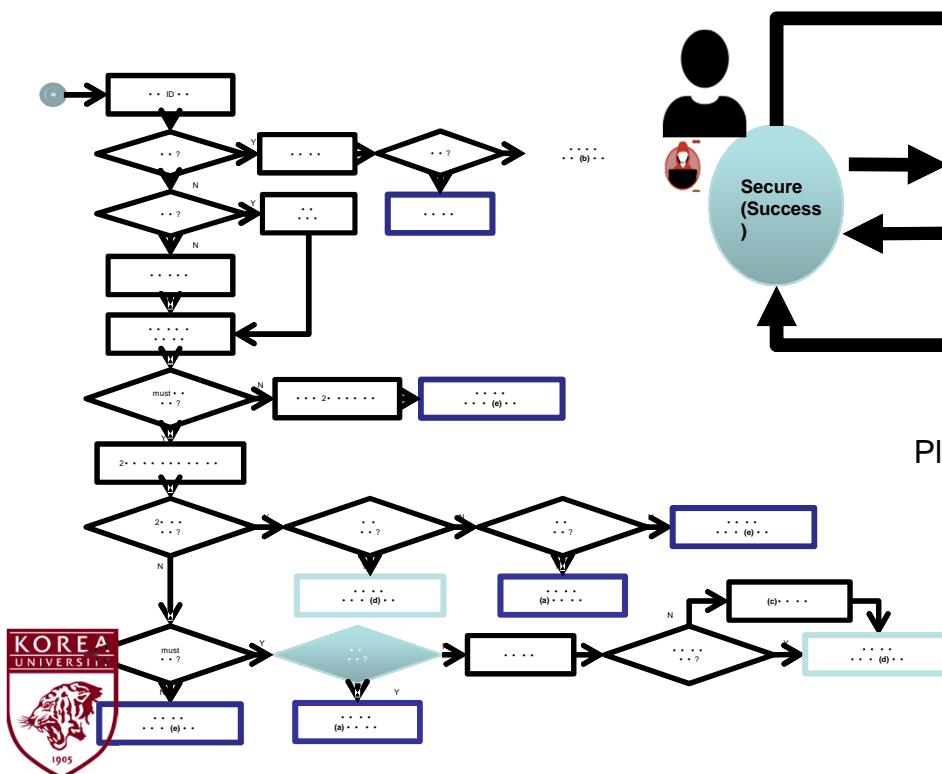
Not a classified slide ;)



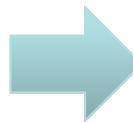
* Work in progress. To be further refined/verified

Preventive Actions

- § It is crucial to effectively estimate, based on patterns of failed login attempts
 - which “element” of the password might have been compromised
 - system might choose to ask text password associated with specific image



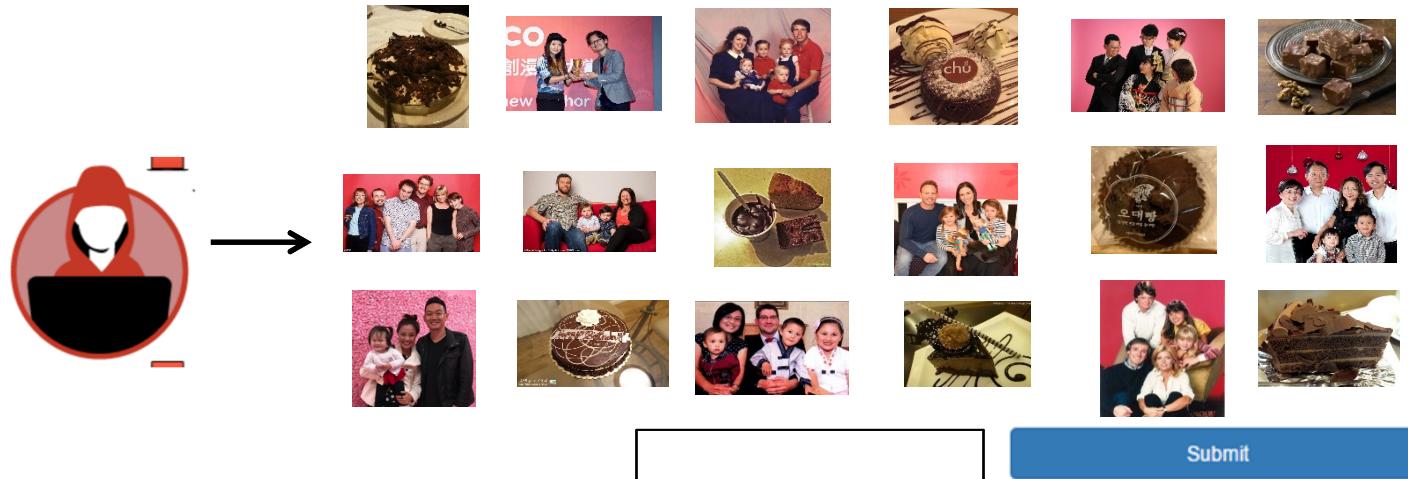
Please update the following password



Dr.* • •



Attack Scenario (2): Automated Attacker



- § Bots are assumed to be equipped with deep learning algorithms, access to powerful search engines, “private” database on actions taken on past failures, etc
- § Most powerful and nasty attack scenarios imaginable are to be investigated



Current Status

- § Implement a prototype system and perform preliminary user study
 - Ease of use
 - Successful Recall: 1) Image, and 2) Texts
 - Failure Analysis
- § Simulate “social engineering” attacks
- § Simulate automated/nasty attacks
- § ...



Conclusions

- § Combine the best of both image and text based authentications
 - Built-in password attack and leak detection mechanisms via trap images
 - Highly personalized association between user 's own images and text labels
 - Easier to create and remember passwords on multiple sites
- § Guidelines to enhance security strength and defeat face recognition algorithms?
 - Self image discouraged, ...
- § Plan to develop to become secure, scalable (e.g., multi-site), easy-to-use two factor authentication



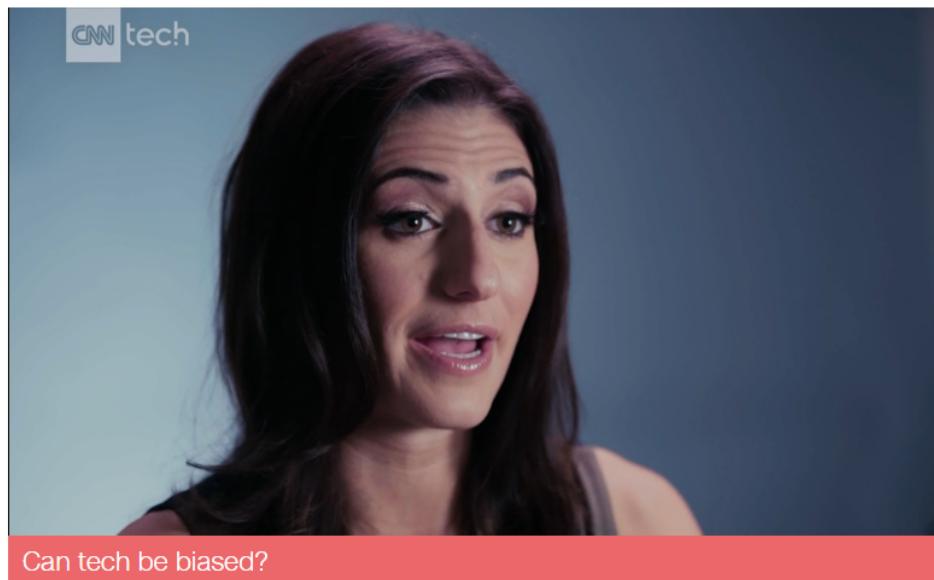
Work Transformed

Beyond passwords: Companies use fingerprints and digital behavior to ID employees

by Selena Larson @selenalarson

🕒 March 18, 2018: 3:53 PM ET

Recommend 686



More companies are ditching passwords and using fingerprints and other biometrics to stop hackers.

"We're seeing a very rapid evolution from what used to be passwords, then smart cards, and now to biometrics," said Alex Simons, director of program management in Microsoft's identity division.

Biometric authentication uses face, fingerprint or iris scans to quickly confirm a person's identity. You probably already use itap by touching the home button to unlock your phone.

IN ASSOCIATION



Advertisement

Investing

Open a New Bank Account



Sponsors of GO Banking Rates

Paid Content

Unfortunately...

Google fingerprint theft

All Images News Videos Shopping More Settings Tools

About 2,250,000 results (0.27 seconds)

Fingerprint theft points to digital danger | Financial Times
<https://www.ft.com/content/446ac29a-dbc1-11e6-9d7c-be108f1c1dce> ▾
Jan 16, 2017 - For public figures, the wealthy and those of interest to intelligence agencies, however, fingerprint theft is already a risk. "The thing to worry ...

Biometric Mythbusters: Do Stolen Fingerprints Mean Identity Theft ...
<https://www.veridiumid.com/.../biometric-mythbusters-stolen-fingerprints-mean-identi...> ▾
Feb 6, 2018 - This article focuses on the theft of a complete fingerprint image. Stay tuned for a follow-up article on why you also don't need to worry to much if ...

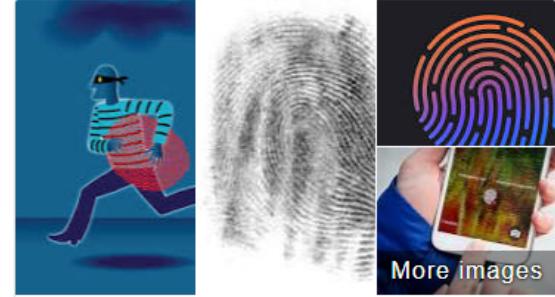
Biometric Identification and Identity Theft - The Balance
[https://www.thebalance.com/.../Personal Finance/Identity Theft/Prevention Practices](https://www.thebalance.com/.../Personal%20Finance/Identity%20Theft/Prevention%20Practices) ▾
Apr 7, 2018 - Some experts call biometrics the answer to identity theft. ... CSI and NCIS employ biometric ID methods to access fingerprints, facial recognition, ...

Videos

Japanese researchers warn of fingerprint theft from 'peace' signs in ...
tnews YouTube - Jan 17, 2017

'Peace' signs risk fingerprint theft, says Japanese study
Reuters - Jan 16, 2017

Your Fingerprints can be Stolen, Copied, and Used from just a Picture
Sling and Stone YouTube - Jan 20, 2017


More images

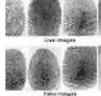
Fingerprint Theft

Peace signs flashed on social media can give hackers access to bank accounts, warn Japanese scientists who have used a digital camera to **steal fingerprint data**. ... "Once you share them on social media then they're gone. Unlike a password you can't change your fingers, so it's information you have to protect."

Fingerprint theft points to digital danger | Financial Times
Financial Times

People also search for

 Fingerprint Mug

 Fingerprint Forgery

 Fingerprint Software

Feedback

"Dangerous Cyber World"

Secure | <https://www.ft.com/content/446ac29a-dbc1-11e6-9d7c-be108f1c1dce>

Apps For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

≡ ⌂ HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Fingerprint theft points to digital danger

Japanese scientists fool biometric security system with off-the-shelf camera



Security risk: a Japanese woman makes a V sign last week at a Tokyo amusement park © Reuters

Robin Harding in Tokyo JANUARY 16, 2017

□ 4

Peace signs flashed on social media can give hackers access to bank accounts, warn Japanese scientists who have used a digital camera to steal fingerprint data.