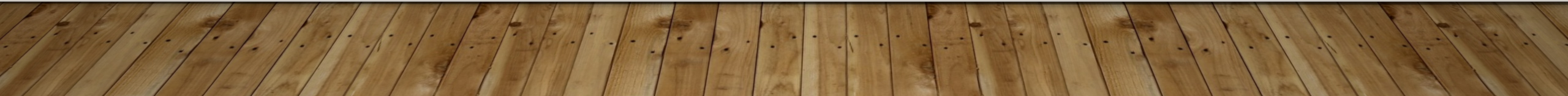


PRACTICAL PASSWORD AUTHENTICATION

ACCORDING TO NIST DRAFT 800-63B

MOTIVATION



DATABASE LEAKAGE

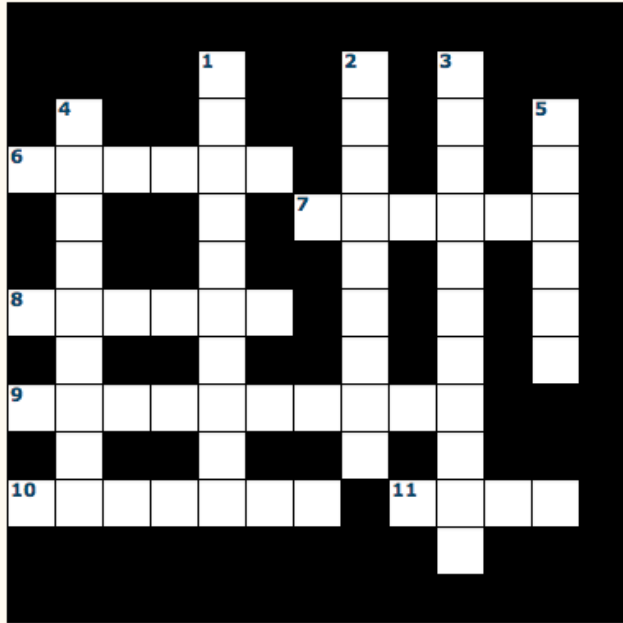
ADOBE

- 152,982,479
- Encrypted with 3DES ECB
 - Same password == same ciphertext

```
4464 ① User ID yahoo.com|-g2B6PhWEH36 ⑤ Password hint try: qwerty123 --
4465-|--|-xxxxx@jcom.home.ne.jp|-Eh5tLomK+N+82csoVwU9bw==|-?????|--
4466-|--|-xx@hotmail.com|-ahw2b2BELzgRTWYvQGn+kw==|-quiero a...|--
4467-|--|-xxx@yahoo.com|-leMTcMPEPcjioxG6CatHBw==|-|--
4468-|username ② Username pe.com|-2GtbVrmsERzioxG6CatHBw==|-|--
4469-|--|-xxxxx@yahoo.com|-4LSlo772tH4= ④ Password data (base64) |
4470-|--|-xxx@hotmail.com|-xxxxx5bZKXpJoxG6CatHBw==|-|--
4471-|--|-xxxx@yahoo.com ③ Email address xG6CatHBw==|-myspace|--
4471-|--|-xxx@hotmail.com|-kby1918wDrrioxG6CatHBw==|-regular|--
```

A crossword based on the Adobe password leak. Inspired by xkcd #1286: Encryptic

Password popularity: **1-100** 101-200 201-300 301-400 401-500 501-600 601-700 701-800 801-900 901-1000



Reveal Check Hide

Across

▼ 6: zk8NJgAOqc4=

dog; cat; pet; dark; dogs name;
Dog; my dog; black dog; dog name;
dog's name; darkness; black cat;
sonic; black; kitty; horse; Cat; pets
name; sombra; puppy; cats name;
old dog; shade; first dog; pet name;
doggy; hedgehog; cat's name; bike;
my cat; nickname; Pet; me; light;
favorite pet; usual; sha; doggie;
pet's name; first pet; animal; sh;
shad; s; car; first cat; Dog's name;
chien; favorite dog; ombre

► 7: WIMTLimQ5b4=

► 8: FTeB5SkrOZM=

► 9: WqflwJFYW3+PszVFZo1Ggg==

► 10: yxzNxPlsFno=

► 11: L3uQHNDf6Mw=

Down

▼ 1: 2aZl4Ouarwm52NYYI936YQ==

adobe; adobex2; adobe2; adobe
twice; twice; adobetwice; adobe2x;
site; ??????; name; software; 2x;
company; 2xadobe; programa;
adobe x 2; program; adobe x2; ???;
ad; adobe*2; ???; Adobe; double;
namename; 2adobe; ?????; x2; a;
name twice; photoshop; company
name; adobe adobe; adobe?; ado;
aa; company twice; 2; marca;
website; none; adobe 2x; product;
company name twice; adobeX2;
this; logiciel; ??; ???????; what is
this

► 2: L8qbAD3jl3jSPm/keox4fA==

► 3: 7Z6uMyq9bpxe1EB7HjirBQ==

► 4: vp6d18mfGL+5n2auThm2+Q==

► 5: dA8D8OYD55E=

DATABASE LEAKGE

ASHLEY MADISON

- 36 million potential passwords
- Passwords are hashed – bcrypt\$2a\$
 - Legacy code stored `md5(strtolower($username). ':: ' . strtolower($password));`

Device #1: GeForce GTX 1060 6GB, 1536/6144 MB allocatable, 10MCU

Hashtype: MD5

Speed.Dev.#1.: 11560.2 MH/s (95.88ms)


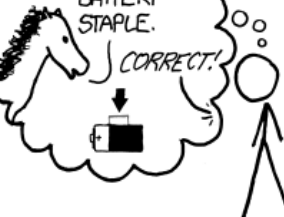
Hashtype: SHA1

Speed.Dev.#1.: 4428.1 MH/s (96.34ms)

Hashtype: bcrypt, Blowfish(OpenBSD)

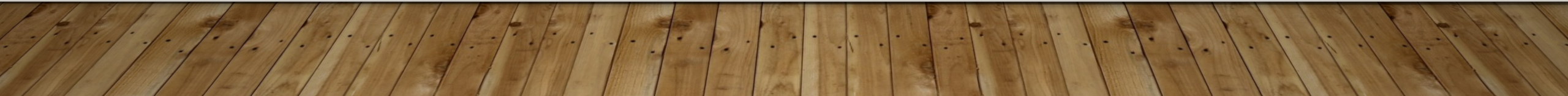
Speed.Dev.#1.: 6631 H/s (46.70ms)

USABILITY PASSWORD RULES

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

TOWARDS BETTER PASSWORDS



SP 800-063-3 PUBLIC COMMENT PERIOD

Digital Identity Guidelines: Public Comment Period Closed

May 2, 2017

The Trusted Identities Group (TIG) thanks all that contributed to the public comment period. We are now in the process of final edits. Please stay tuned for a final version in the near future. Thanks!!!!

Meanwhile, you can find links to the volumes of draft SP 800-63-3 below.



SP 800-63-3

Digital Identity Guidelines



SP 800-63A

Enrollment & Identity Proofing



SP 800-63B

Authentication & Lifecycle Management



SP 800-63C

Federation & Assertions

AUTHENTICATOR ASSURANCE LEVELS

Requirement	AAL1	AAL2	AAL3
Permitted authenticator types	Memorized Secret; Look-up Secret; Out of Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or memorized secret plus: <ul style="list-style-type: none">• Look-up Secret• Out of Band• SF OTP Device• SF Crypto Software• SF Crypto Device	MF Crypto Device SF Crypto Device plus Memorized Secret
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; shall use both authentication factors
MitM resistance	Required	Required	Required
Verifier impersonation resistance	Not required	Not required	Required
Verifier compromise resistance	Not required	Not required	Required
Replay resistance	Not required	Required	Required

AUTHENTICATOR TYPES

- Memorized Secrets
- Look-up Secrets
- Out-of-Band Devices
- Single-factor OTP Device
- Multi-factor OTP Devices
- Single-factor Cryptographic Software
- Single-factor Cryptographic Devices
- Multi-factor Cryptographic Software
- Multi-factor Cryptographic Devices

MEMORIZED SECRET AUTHENTICATORS

A Memorized Secret authenticator (commonly referred to as a *password* or, if numeric, a *PIN*) is a secret value that is intended to be chosen and memorable by the user.

Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value.

MEMORIZED SECRETS

MINIMUM LENGTH

OLD

- 6 characters/4 random digit PIN (LOAI)
- 8 characters/6 random digit PIN (LOA 2)

NEW

- SHALL be at least 8 characters or 6 random digits

MEMORIZED SECRETS MAXIMUM LENGTH

OLD

- None

NEW

- SHALL accept at least 64 characters
- No truncation

MEMORIZED SECRETS

SPACE CHARACTERS

OLD

- None

NEW

- SHALL accept space characters
- MAY canonicalize them out

MEMORIZED SECRETS CHARACTER SET

OLD

- Alphabet

NEW

- SHALL accept printable ASCII characters
- SHOULD accept Unicode characters, including emojiis

MEMORIZED SECRETS

PASSWORD HINT

OLD

- none

NEW

- SHALL NOT store password hint
- SHALL NOT prompt for specific type of information e.g. „Name of first pet“

MEMORIZED SECRETS THROTTLING

OLD

- SHALL limit to 100 authentication attempts in 30-day period
- MAY use captchas, delays, IP blacklisting

NEW

- SHALL implement a throttling mechanism
- SHALL effectively limit online attackers to no more than 100 consecutive failed attempts on a single account

MEMORIZED SECRETS

PASSWORD COMPOSITION

OLD

- Constrain user-generated secret

NEW

- SHOULD NOT impose constraints
- SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised

MEMORIZED SECRETS

PASSWORD COMPOSITION - DICTIONARIES

- What dictionary?
 - rockyou.txt
- How does the user react?
 - 1234567
- zxcvbn: realistic password strength estimation

MEMORIZED SECRETS VERIFIER STORAGE

OLD

- SHALL NOT store plaintext
- MAY salt and encrypt

NEW

- SHALL store memorized secrets in a form that is resistant to offline attacks
- SHALL be hashed with a *salt* value using an approved hash function such as PBKDF2
- salt value SHALL be a 32-bit or longer random value generated by an approved random bit generator
- SHOULD at least 10000 iterations of the hash function
- SHOULD utilized a keyed hash function (HMAC)

MEMORIZED SECRETS

DISPLAYING SECRETS

OLD

- None

NEW

- SHOULD offer option to display secret in clear text

MEMORIZED SECRETS EXPIRATION

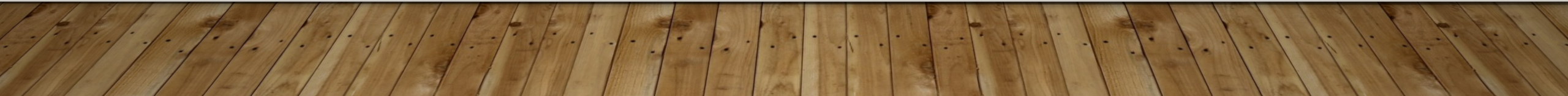
OLD

- None

NEW

- SHOULD NOT require being changed unless compromised

LIFE AFTER PASSWORDS



IS THERE A LIFE AFTER PASSWORDS?

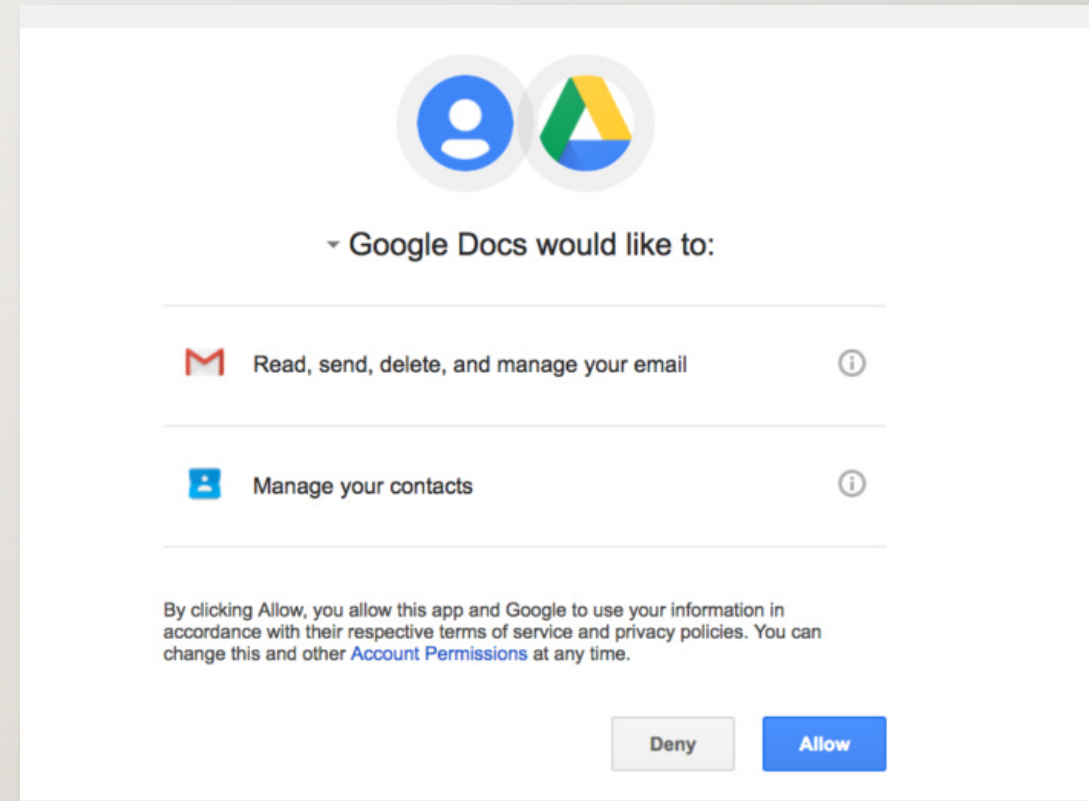
ALTERNATIVES

- NFC
- YubiKey
- Password Managers
- Biometrics

IS THERE A LIFE AFTER PASSWORDS?

PHISHING ATTACKS

- OAuth Token



LOOK-UP SECRETS

A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. For example, a claimant may be asked by the verifier to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of look-up secrets is the use of "recovery keys" stored by the subscriber for use in the event another authenticator is lost or malfunctions.

OUT-OF-BAND DEVICES

An out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel that is separate from the primary channel for e-authentication. The out-of-band authenticator can operate in one of the following ways:

- The claimant transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the claimant may receive the secret on their mobile device and type it (typically a 6-digit code) into their authentication session.
- The claimant transfers a secret received via the primary channel to the out-of-band device for transmission to the verifier via the secondary channel. For example, the claimant may view the secret on their authentication session and either type it into an app on their mobile device or use a technology such as a barcode or QR code to effect the transfer.
- The claimant compares secrets received from the primary channel and the secondary channel and confirms the authentication via the secondary channel.
- The purpose of the secret is to securely bind the authentication operation on the primary and secondary channel. When the response is via the primary communication channel, the secret also establishes the claimant's control of the out-of-band device.

SINGLE-FACTOR OTP DEVICE

A single-factor OTP device generates OTPs. This includes hardware devices as well as software-based OTP generators installed on devices such as mobile phones. This device has an embedded secret that is used as the seed for generation of OTPs and does not require activation through a second factor. The OTP is displayed on the device and manually input to the verifier, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. A single-factor OTP device is *something you have*.

Single-factor OTP devices are similar to look-up secret authenticators with the exception that the secrets are cryptographically and independently generated by the authenticator and verifier and compared by the verifier. The secret is computed based on a nonce that may be time-based or from a counter on the authenticator and verifier.

HONORABLE MENTIONS

SESSION MANAGEMENT

Once an authentication event has taken place, it is often desirable to allow the user to continue using the application across multiple subsequent interactions without requiring the user to repeat the authentication event every time.

SESSION MANAGEMENT

BROWSER COOKIES

- SHALL be tagged to be accessible only on secure (HTTPS) sessions.
- SHALL be accessible to the minimum practical set of hostnames and paths.
- SHOULD be tagged to be inaccessible via JavaScript (HttpOnly).
- SHOULD be tagged to expire at or soon after the validity period of the session. This requirement is intended to limit the accumulation of cookies, but SHALL NOT be depended upon to enforce session timeouts.

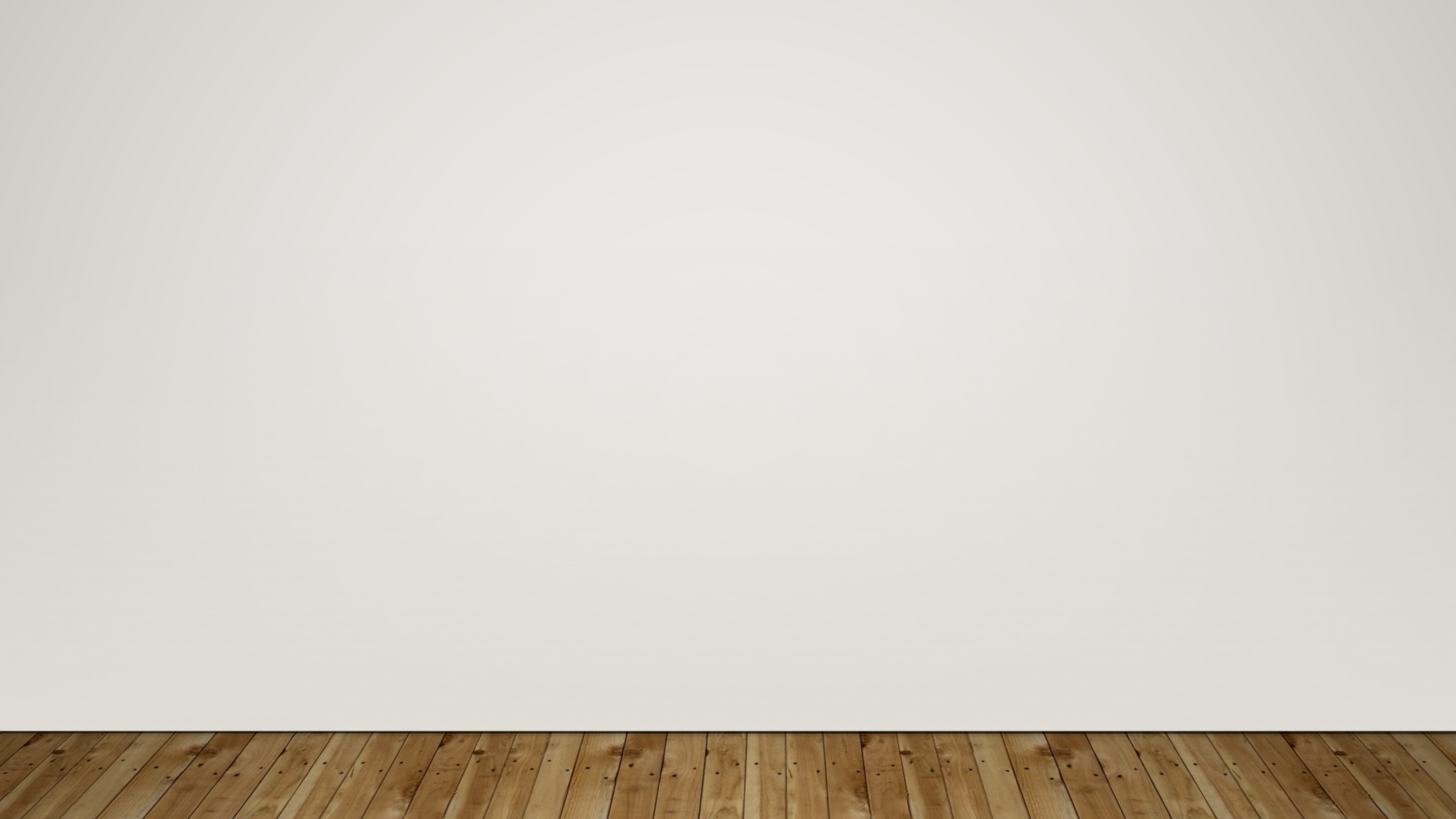
USABILITY CONSIDERATIONS

A user's goal for accessing an information system is to perform an intended task; authentication is the task that enables this goal. However, from the user's perspective, authentication stands between them and their intended task. Effective design and implementation of authentication makes it easy to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens.

USABILITY CONSIDERATIONS MEMORIZED SECRETS

Usability considerations for typical usage include:

- Memorability of the memorized secret.
 - The likelihood of recall failure increases as there are more items for users to remember; with fewer memorized secrets, users can more easily recall the specific memorized secret needed for a particular RP. The memory burden is greater for a less frequently used password.
- User experience during entry of the memorized secret.
 - Support copy and paste functionality in fields for entering memorized secrets, including passphrases.



LINKS

- <https://pages.nist.gov/800-63-3/>
- https://www.slideshare.net/jim_fenton/toward-better-password-requirements
 - <https://www.youtube.com/watch?v=nXg-kh7fKEE>
- <https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/>
- <https://auth0.com/blog/what-the-new-nist-guidelines-mean-for-authentication/>