

Authentication



<https://twitter.com/ofureonline/status/1512090899622379520>

Patch Notes

We **do** have recitation tomorrow (finally)!

- Recitations are not streamed or recorded

Authentication and Authorization

Authentication (AuthN): Who someone is



Authentication and Authorization

Authentication (AuthN): Who someone is

Authorization (AuthZ): What someone is allowed to do

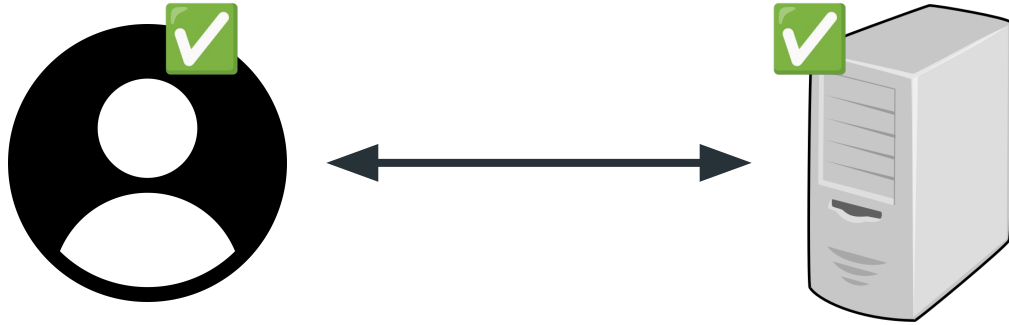




Authentication

Authentication (AuthN)

Authentication: How can we prove that somebody is who they claim to be?



Authentication (AuthN)

We require users to show us something that only they should know or have

Federated Identity Service

Log in to CU Portal

IdentiKey Username (example: chbu1234)

IdentiKey Password

[Log In](#) [Advanced Settings...](#)



Authentication (AuthN)

Something only they **know**

- Password, security questions

Something only they **have**

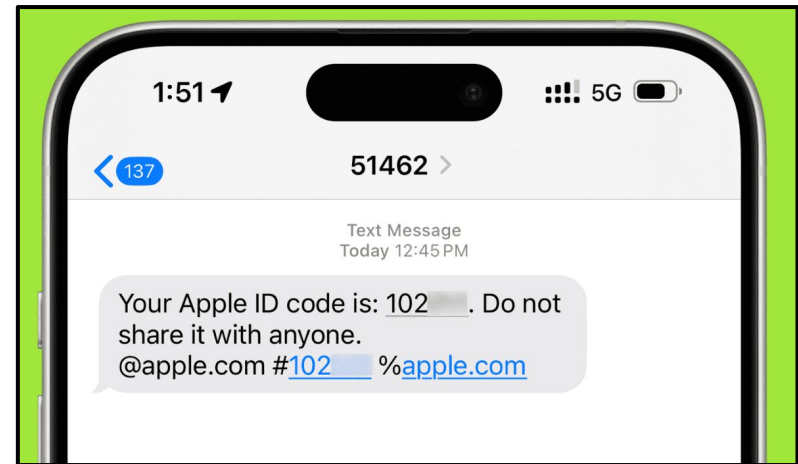
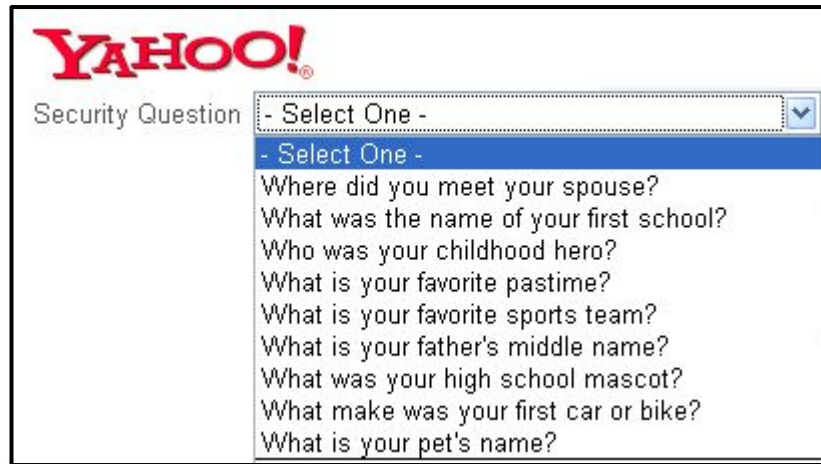
- Text code, ID card, email account

Something only they **are**

- Fingerprint, face ID

Authentication (AuthN)

Different authentication methods are harder to learn, guess, or acquire



Authentication (AuthN)

Former SolarWinds CEO blames intern for 'solarwinds123' password leak



By [Brian Fung](#) and [Geneva Sands](#), CNN

Updated 5:34 PM ET, Fri February 26, 2021



MORE FROM CNN



Eminem takes a
halftime perform



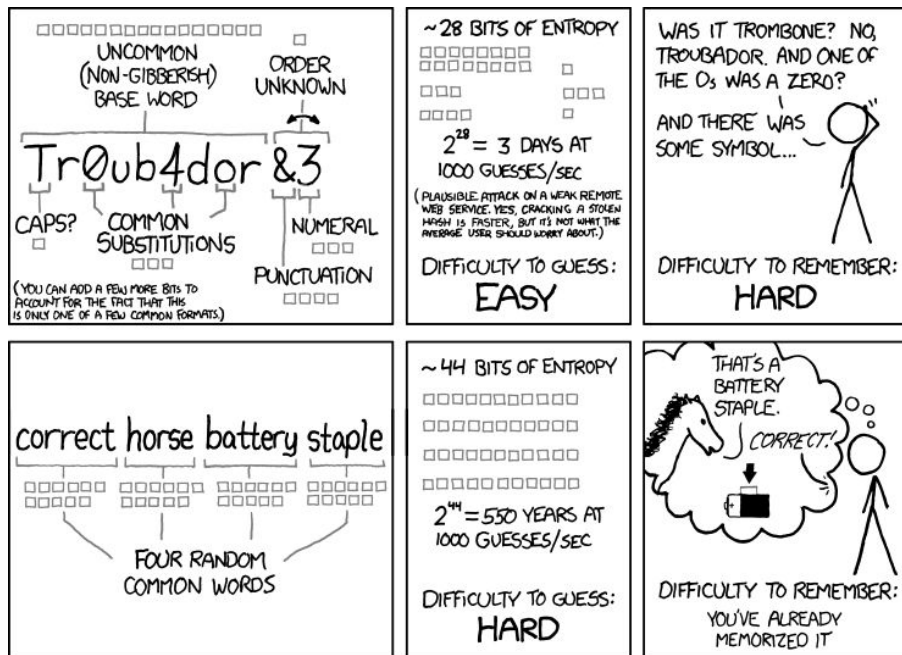
Eminem took a
Super Bowl half

Authentication (AuthN)

Entropy: A measure of “randomness”, in security this is the number of possible options for a value

- 4-digit PIN: $\sim 2^{14}$ Possibilities
- 16 character password with letters, numbers, and symbols: $\sim 2^{96}$ Possibilities

Authentication (AuthN)



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.

Authentication (AuthN)

A lot of common passwords are even worse...

Passwords

Top 100

1. 123456	21. qwertyuiop	41. asdfgh	61. 112233	81. princess
2. password	22. 123321	42. hunter	62. george	82. joshua
3. 12345678	23. mustang	43. buster	63. asshole	83. cheese
4. qwerty	24. 1234567890	44. soccer	64. computer	84. amanda
5. 123456789	25. michael	45. harley	65. michelle	85. summer
6. 12345	26. 654321	46. batman	66. jessica	86. love
7. 1234	27. pussy	47. andrew	67. pepper	87. ashley
8. 111111	28. superman	48. tigger	68. 1111	88. 6969
9. 1234567	29. 1qaz2wsx	49. sunshine	69. zxcvbn	89. nicole
10. dragon	30. 7777777	50. iloveyou	70. 555555	90. chelsea

Authentication (AuthN)

On the web, we typically use cookies to authenticate:

```
POST /messages/new HTTP/1.1
```

```
Host: www.google.com
```

```
Cookies: username=alex
```

```
message:Hi!
```

Authentication (AuthN)

Terribly insecure: Cookie is just the username, user ID, or something easy to guess

Authentication (AuthN)

Terribly insecure: Cookie is just the username, user ID, or something easy to guess

Better: Cookie is a long, random string and the server keeps a mapping of cookie/username values

```
{  
  "7ce5a141-6431-4d83-8913-25447d35e7a0": "alex",  
  "d4622f93-59b2-4a49-a104-39af77a01cc0": "admin",  
}
```




[Demo: Secure cookies]

Authentication (AuthN)

Secure cookies demo code:

```
import random
from flask import Flask, redirect, render_template, request

app = Flask(__name__)

cookie_map = {}

@app.route("/")
def index():
    cookie = request.cookies.get("logged_in_as")
    current_user = cookie_map.get(cookie)

    return render_template("index.html", current_user=current_user)

@app.route("/login", methods=["GET"])
def login_get():
    return render_template("login.html")

@app.route("/login", methods=["POST"])
def login_post():
    username = request.form["username"]
    password = request.form["password"]

    if username == "alex" and password == "swordfish":
        cookie = random.randbytes(20).hex()
        cookie_map[cookie] = "alex"

        response = redirect("/")
        response.set_cookie("logged_in_as", cookie)
        return response

app.run(debug=True)
```

```
<!-- index.html -->
<h1>Example Site</h1>

<p>Logged in as: {{ user }}</p>

<a href="/login">Login</a>

<!-- login.html -->
<h1>Example Site</h1>

<form action="/login" method="post">
    Username:
    <input type="text" name="username">

    Password:
    <input type="password" name="password">

    <input type="submit">
</form>

<form action="/login" method="post">
    <input type="text" name="username">
</form>
```



Why not use the password as a cookie?



Multi-Factor Authentication

Authentication (AuthN)

Multi-factor Authentication (MFA): Requiring more than one authentication method

(Also referred to as Two-factor Authentication, or 2FA)


Log in to CU Portal

IdentiKey Username (example: chbu1234)

IdentiKey Password


[Log In](#) [Advanced Settings...](#)





Use your security key

Verify it's you by using your security key...



[Other options](#)

[Need help?](#) Secured by Duo



Why use multiple forms of authentication?

Authentication (AuthN)

More authentication methods makes it much harder to steal *all* of them!

Google account hacks dropped by half after pushing two-step authentication by default

The results support an ongoing project to boost enrollment for additional security measures

By **Corin Faife** | @corintxt | Feb 8, 2022, 12:27pm EST



SHARE



Authentication (AuthN)

More authentication methods makes it much harder to steal *all* of them!

- Food for thought: Why stop at 2FA? Why not 3FA, etc?

Google account hacks dropped by half after pushing two-step authentication by default

The results support an ongoing project to boost enrollment for additional security measures

By [Corin Faife](#) | [@corintxt](#) | Feb 8, 2022, 12:27pm EST

[f](#) [t](#) [SHARE](#)



Have a nice weekend!



Joyce Carol Oates ✓
@JoyceCarolOates

Lilith is in a perpetual state of anxiety because when it is demanded of her that she "authenticate" herself she has no cell phone upon which to receive a special code; thus, like the man without a country, she has no identity, she is shunned by all authenticated persons.



<https://x.com/JoyceCarolOates/status/1958897231437631579>

Alex Curtiss | CSCI 3403