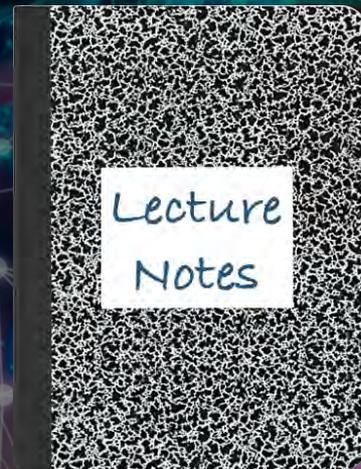


CS 419: Computer Security

Week 13: Part 1
CAPTCHA

Paul Krzyzanowski



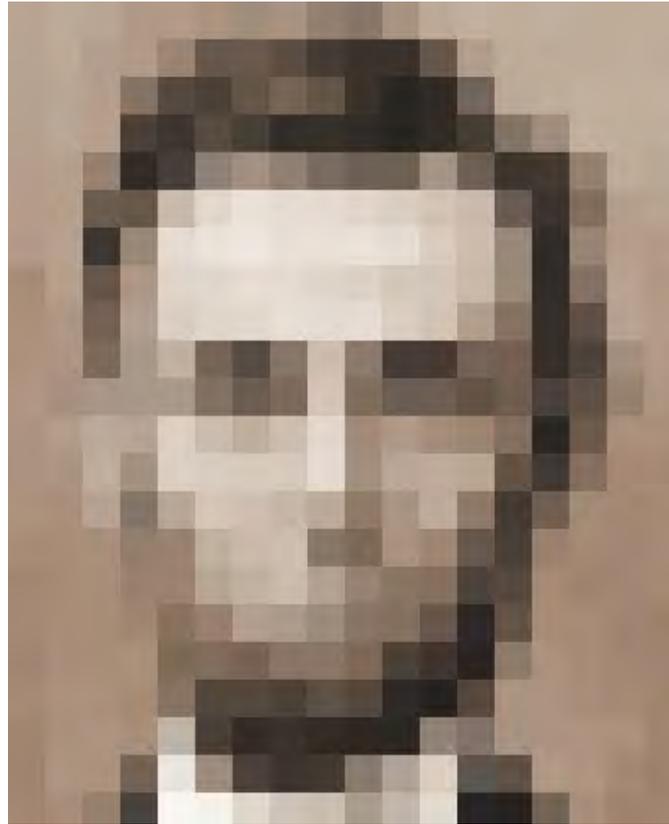
© 2022 Paul Krzyzanowski. No part of this content, may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

CAPTCHA: Detecting Humans

Gestalt Psychology (1922-1923)

- **Max Wertheimer, Wolfgang Köler, Kurt Koffka**
- **Laws of organization**
 - Proximity
 - We tend to group things together that are close together in space
 - Similarity
 - We tend to group things together that are similar
 - Good Continuation
 - We tend to perceive things in good form
 - Closure
 - We tend to make our experience as complete as possible
 - Figure and Ground
 - We tend to organize our perceptions by distinguishing between a figure and a background

Gestalt Psychology



18 x 22 pixels

Objects on Mars?



Elvis

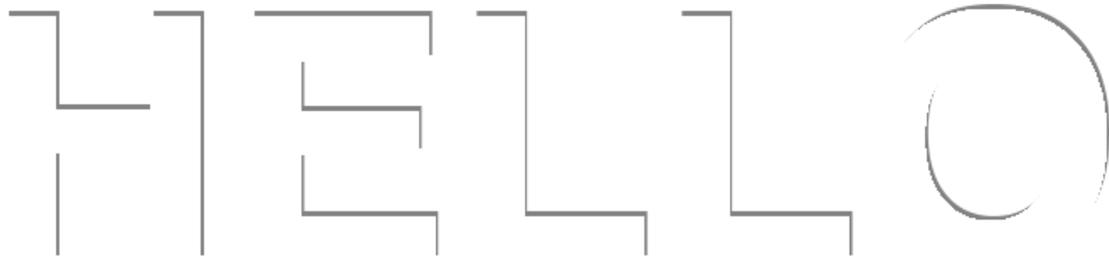


Face



Female statue

Gestalt Psychology: text continuity



HELLO

HELLO

Authenticating humanness

Battle the Bots

- Create a test that is easy for humans but extremely difficult for computers

CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

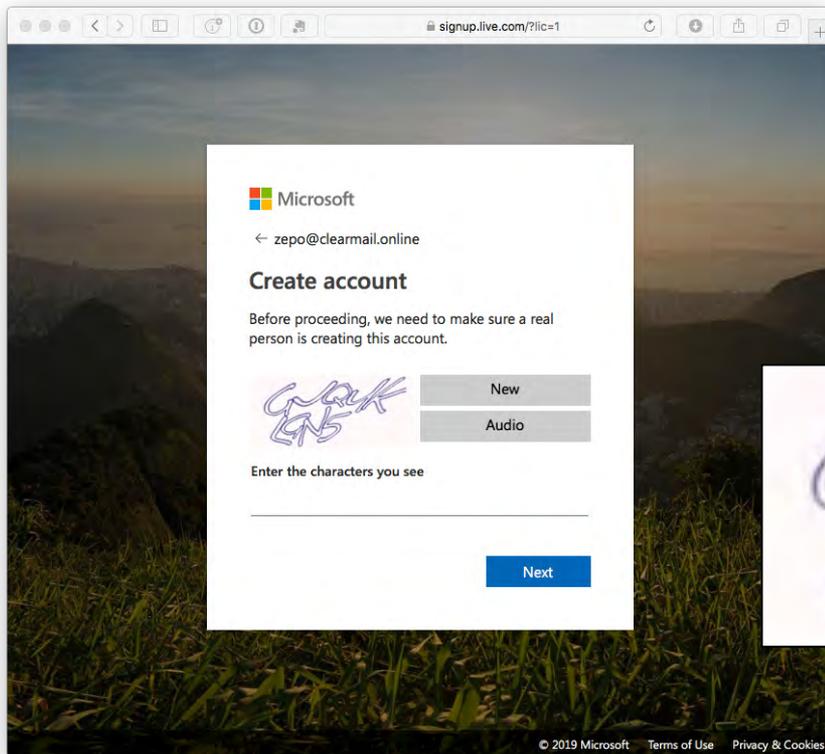
- Image Degradation
 - Exploit our limits in OCR technology
 - Leverages human Gestalt psychology: reconstruction

Origins

- 1997: AltaVista – prevent bots from registering URLs with the search engine
- 2000: Yahoo! and Manuel Blum & team at CMU
 - EZ-Gimpy: one of 850 words
- Henry Baird @ CMU & Monica Chew at UCB
 - BaffleText: generates a few words + random non-English words

CAPTCHA Example (2019)

Microsoft



See captchas.net

They're getting harder

Name

E-mail Address

Password Confirm Password

Please type captcha here 562  

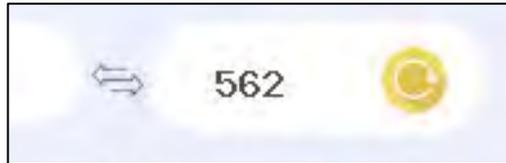
(Optional) Please enter your phone number if you'd like us to call you to explain our products and services.

Select Country Code Phone Number

I'd like to receive email about product updates, personalized recommendations, offers, and PowerPoint and presentation tips and tricks.

SIGN UP

By Pressing "Sign up" you accept our [Privacy Policy](#)



Microsoft account

Help us make sure you're not a robot

Enter the characters you see
[New](#) | [Audio](#)



Send me email with promotional offers from Microsoft. (You can unsubscribe at any time.)

Click **I accept** to agree to the [Microsoft services agreement](#) and [privacy & cookies statement](#).

I accept



 Microsoft

← zepo@clearmail.online

Create account

Before proceeding, we need to make sure a real person is creating this account.



Enter the characters you see

Next



Problems

- **Accessibility**

- Visual impairment → audio CAPTCHAs
- Deaf-blind users are left out

- **Frustration**

- OCR & computer vision has improved a lot!
- Challenges that are difficult for computers may be difficult for humans

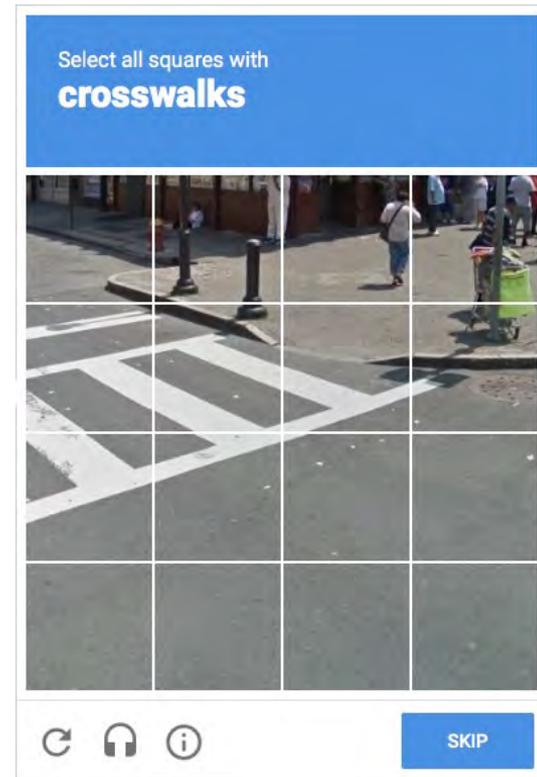
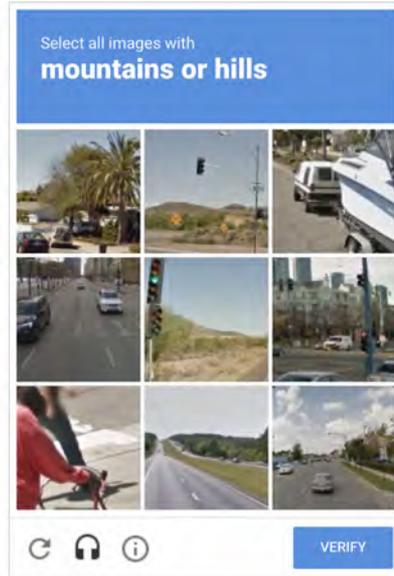
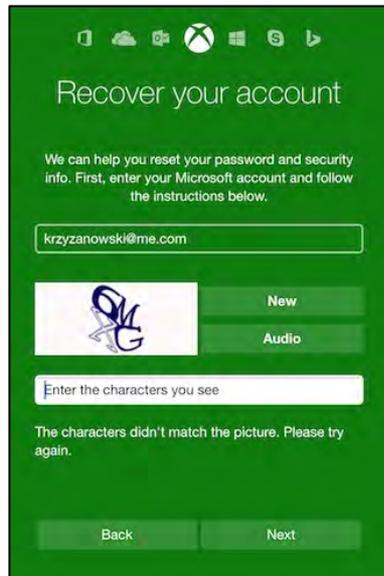
- **Attacks**

- Man in the middle attacks
 - Use human labor – CAPTCHA farms
- Automated CAPTCHA solvers
 - Initially, educated guesses over a small vocabulary

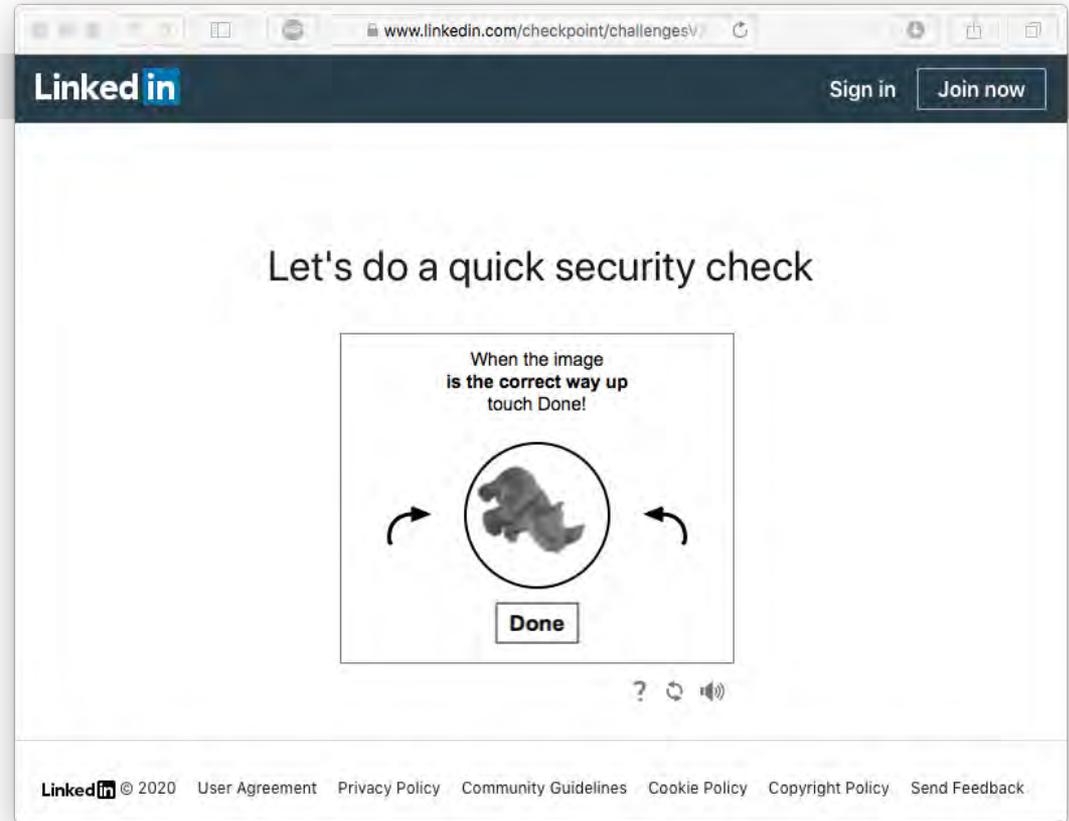
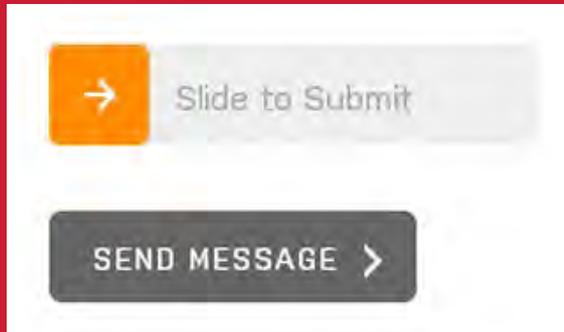


Alternate approaches

- **MAPTCHAs = math CAPTCHAs**
 - Solve a simple math problem
- **Puzzles, scene recognition**



Alternate approaches



reCAPTCHA

Ask users to translate images of real words & numbers from archival texts

- Human labor fixed up the archives of the New York Times

Two sections

(1) known text

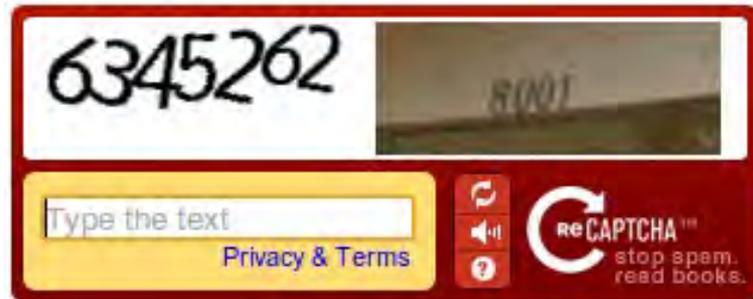
(2) image text

- Assume that if you get one right then you get the next one correct
 - Try it again on a few other people to ensure identical answers before marking it correct

Google bought reCAPTCHA 2009

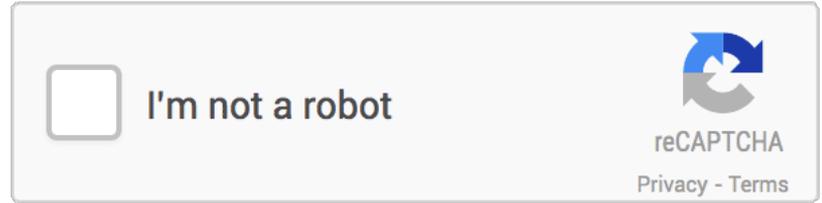
- Used free human labor to improve transcription of old books & street data

2014: Google found that AI could crack CAPTCHA & reCAPTCHA images with 99.8% accuracy



NoCAPTCHA reCAPTCHA

Just ask users if they are a robot



- **Reputation management**

- “Advanced Risk Analysis backend”
- Check IP addresses of known bots
- Check Google cookies from your browser
- Considers user’s engagement with the CAPTCHA: before, during, and after
 - Mouse movements & acceleration, precise location of clicks

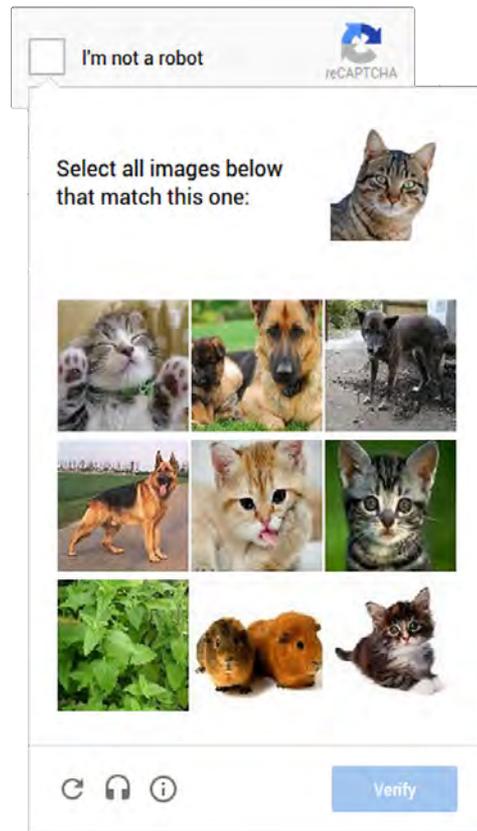
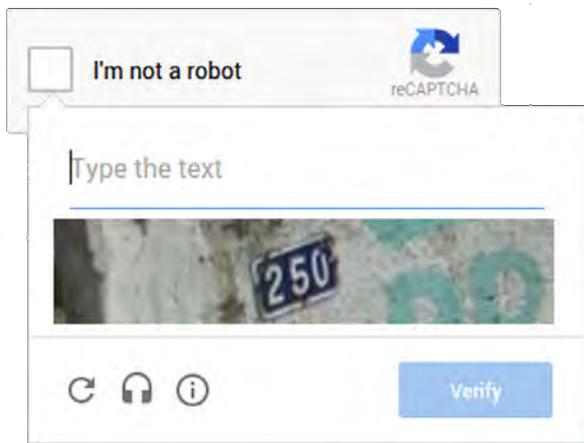
- **Latest version: invisible reCAPTCHA**

- Don’t even present a checkbox

NoCAPTCHA fallback

If risk analysis fails,

- Present a CAPTCHA
- For mobile users, present an image identification or labeling problem



Other approaches: Text/email verification

- **Text/email verification**

- Ask users for a phone # or email address
- Similar to two-factor authentication but we're not authenticating the user
- Service sends a message containing a verification code
 - Still susceptible to spamming & automation
 - Makes the process more cumbersome
 - Requires users to disclose some information

- **Measure form completion times**

- Users take longer than bots to fill out and submit forms
- Measure completion times
 - Bots can program delays if they realize this is being done

The End