Rethinking Passwords

Bill Cheswick

ches@cheswick.com

https://cheswick.com/ches/talks

THE MENTOR PROJECT®

https://mentorproject.org

Corona Savings and Loan

The Trusting Bank: no Passwords!

Est. 2020.

© Alson Wong

Corona Savings and Loan

The online bank with easy passwords!
Est. 2020.

© Alson Wong

Easy Passwords

- A single digit, 1—8
- No password guessing, with our new dynamite chairs!

Our (stupid) password file

```
Liam    4
Noah    8
William 3
James   1
Oliver  4
Emma    4
Olivia  5
Ava     8
Isabel  4
Sophia  1
```

- **Stupid because we (and a hacker) can see the password if we get access to this file.**

Password plus a hash

Liam	4	c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Noah	8	4e0fc5cb9862ef52f5256ca8cbcb9519929ee3a08595f2b3508659e80ddb9293
William	3	d07168bd799f53e50d1a1c390773fa503669048353bb3a8dd8bc17f93dcd82dd
James	1	e66cb464b78b3dbe293eb17eb15ac77b21a4c73c712205a807777f6a0f117682
Oliver	4	c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Emma	4	c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Olivia	5	56b2a716f92160eeabded2dcc3f1fe6e5e7eed11ad7ae48d6ce9a35ac615391c
Ava	8	4e0fc5cb9862ef52f5256ca8cbcb9519929ee3a08595f2b3508659e80ddb9293
Isabel	4	c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Sophia	1	e66cb464b78b3dbe293eb17eb15ac77b21a4c73c712205a807777f6a0f117682

- **The hash does not show our passwords!**
- **Note: same password, same hash**
- **But we still have passwords, so…**

A much better password file

```
Liam    c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Noah    4e0fc5cb9862ef52f5256ca8cbcb9519929ee3a08595f2b3508659e80ddb9293
William d07168bd799f53e50d1a1c390773fa503669048353bb3a8dd8bc17f93dcd82dd
James   e66cb464b78b3dbe293eb17eb15ac77b21a4c73c712205a807777f6a0f117682
Oliver  c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Emma    c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Olivia  56b2a716f92160eeabded2dcc3f1fe6e5e7eed11ad7ae48d6ce9a35ac615391c
Ava     4e0fc5cb9862ef52f5256ca8cbcb9519929ee3a08595f2b3508659e80ddb9293
Isabel  c1d1429e62f91aceeeca554c7ea4103de81f6119a6b143014308ffa1e20e8d3e
Sophia  e66cb464b78b3dbe293eb17eb15ac77b21a4c73c712205a807777f6a0f117682
```

- **No passwords here**
- **What’s the deal with this ‘hash’ business**

A Hash Function

- **Mathematically chops up the input into a number, a "one-way function," we hope.**
- **It is supposed to be extremely hard to make two different inputs with the same hash.**
- **It is supposed to be extremely hard to compute the original input from the hash alone…**

A Hash example

- hash:
  a1c222d523f615fbee535f2e0a6f86b8955f425c
  b368a5beff14848b57ab853b
- input:
  8159152832478977343456112695961158942
  72000000000
- Where the original input came from: 40!
- (For you technical types, I used a 256-bit HMAC algorithm with the key “Corvid Savings and Loan”)

Marketing and Legal report that the dynamite chairs are problematic

- And we are losing customers
- How about a four digit password?
- Limit to four tries
- No dynamite

My first ATM, c. 1972; FNB of Allentown, Pa

- 4 digit PIN
  - 10,000 possibilities
  - ~13 bits of entropy
- It has worked for >50 years!
- The Europeans have 6 digit PINS
  - (It really doesn’t matter)

Early Wells Fargo ATM

Wells Fargo Archives

It has worked because

- Number of tries is limited by an authentication device in the ATM, and at the bank if online
- After too many tries, the machine eats the card.
- We can guess, but don’t have access to an oracle that gives us unlimited answers....
- There are about a thousand bad PIN choices
  - 1111, 1234, dates

PINS

#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%

#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

http://www.datagenetics.com/blog/september32012/index.html

But what if they get access to our password file?

- Insider attack?
  - The three Bs: burglary, bribery, and blackmail
- This should never happen, but it often does

Passwords chosen at random from 74,000 words

```
Liam    2d166b0fffeb0a86f32d11e19e1dcaa6c9d7884f475178ce8897ff5a290639b7
Noah    99a556dbc1a1aec0d8fe6266c34dbd0236c39b4d1b7cadcfa1843be1337f9112
William 224b5ff4f8bdf71384c9084a95b56741ffa85971627951ae20b531717555498 8
James   0562a111336a0e0c8f960ddc33fdd9a3d3913e6da98e84ab5c7150cd8cbc54d0
Oliver  014cefc3d76c90bf65e2a4d670418ae8f56a5f51201616565 8e1dd859f2aa5c5
Emma    42fda778cc499d94bafa09095875c9f5175dc606d1b268a44cdd860303204 8e7
Olivia  18e9a00962253a9f070e6cdbd8f90e3e867a64aad788a84917b7398d6ae16b52
Ava     292e2c306c038fe18de06ba193ac25a279bf2015818d75caee6ada3477cf6c83
Isabel  bea1b2454ec96a45767fc09e1ecee57c3999ae379552587f9d28a07b96d5c41c
Sophia  6d4ac4ba0844b6426dc5a1f3c66f3aa9f01b5d90826877e72994324d9893761d
```

- **OK attackers, what do you do now?**

The words are

Liam	vermin-footed
Noah	all-divine
William	wet-air pump
James	eaden-soled
Oliver	strawberry fern
Emma	elf-ruin
Olivia	obturator fascia
Ava	bush bean
Isabel	re-ebullient
Sophia	pilot flame

- **Pretty obscure stuff…**

Hashed passwords, from a publicly-available FTP site

```
root:DZo0RWR.7DJuU:0:2:0000-Admin(0000):/:
daemon:*:1:1:0000-Admin(0000):/:
bin:*:2:2:0000-Admin(0000):/bin:
sys:*:3:3:0000-Admin(0000):/usr/v9/src:
adm:*:4:4:0000-Admin(0000):/usr/adm:
uucp:*:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:*:10:10:0000-uucp(0000):/usr/spool/uucp…
ftp:anonymous:71:14:file transfer:/:no soap
research:nologin:150:10:ftp acct:/forget:/it/baby
ches:La9Cr9ld9qTQY:200:1:me:/u/ches:/bin/sh
dmr:laHheQ.H9iy6l:202:1:Dennis:/u/dmr:/bin/sh
rtm:5bHD/k5k2mTTs:203:1:Robert:/u/rtm:/bin/sh
adb:dcScD6gKF./Z6:205:1:Alan:/u/adb:/bin/sh
td:deJCw4bQcNT3Y:206:1:Tom:/u/td:/bin/sh
```

```
root:why:0:2:0000-Admin(0000):/:
daemon:*:1:1:0000-Admin(0000):/:
bin:*:2:2:0000-Admin(0000):/bin:
sys:*:3:3:0000-Admin(0000):/usr/v9/src:
adm:*:4:4:0000-Admin(0000):/usr/adm:
uucp:*:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:*:10:10:0000-uucp(0000):/usr/spool/uucp…
ftp:anonymous:71:14:file transfer:/:no soap
research:nologin:150:10:ftp acct:/forget:/it/baby
ches:are:200:1:me:/u/ches:/bin/sh
dmr:you:202:1:Dennis:/u/dmr:/bin/sh
rtm:wasting:203:1:Robert:/u/rtm:/bin/sh
adb:your:205:1:Alan:/u/adb:/bin/sh
td:time:206:1:Tom:/u/td:/bin/sh
```

A file of password hashes is an oracle we can consult on our own machines

Hasan’s guesses

- (Why does he need to know the password to the cave?)
- He knew it began with an “S”
- He made five guesses in 13 seconds
  - ~277 per hour
- grep -i “^s” /usr/share/dict/words|wc -l
  - 25162
- 25162/277 = 90 hours, about 3.75 days
- (Note: Hasan’s employment agreement includes a “jackal” clause, which is not popular in modern regulatory environments.)

CSC-STD-002-85: DOD Password Management Guideline

- The “green book”.
- A variety of mostly-excellent security suggestions
- Recommended password strength, and password change frequency
- They assumed access to an oracle at 120 characters/second, over a telephone line
- These were reasonable results for the time, but
  - The threat model has changed vastly since 1985

Scheme	Cracked in		Change time	
8 character, full alphanumeric	6.72	mins.	0.40	ms.
8 character, EoN	9.25	days	31.19	ms.
11 character, EoN	20,390	years	7.4	days
13 character, full alphanumeric	906,123	years	331	days
12 character, Eye-of-newt	1,896,229	years	692	days

Dictionary Attacks

- Have a computer try as many password guesses as possible
- The required effort is called the “work factor”, and the resistance to attack is often (incorrectly) called the “entropy” of the password.
- These attacks can be directed at online authentication services, or against stolen hashed password files.

The Dictionary Attack Arms Race

- Moore’s Law: 12 doublings since 1990
- And multi-core CPUs are perfect for password cracking
- Can a human choose and remember a password that a computer can’t guess when limited only by computer speed and time available?
- Guessing rates can be 8 x 10^9 guesses per second per CPU!

Has this been working?

No.

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Year	Entity	Millions of passwords lost
2018	Marriott	500
2017	Equifax	143
2016	Adult Friend Finder	412.2
2015	Anthem	78.8
2014	eBay	145
	JP Morgan Chase	76
	Home Depot	56
2013	Yahoo	3000
	Target	110
	Adobe	38
2012	US OPM	22
2011	Sony's Playstation	77
	RSA security	40
2008	Heartland Payment	134
2006	TJX	94

...and what are the top passwords?

123456.	23.2m
123456789.	7.7m
qwerty.	3.8m
password.	3.6m
1111111	3.1m
12345678	2.9m
abc123	2.8m
1234567	2.5m
password1	2.4m
12345	2.3m
1234567890	2.2m
123123	2.2m
000000	1.9m

Iloveyou	1.6m
1234	1.3m
1q2w3e4r5t	1.2m
Qwertyuiop	1.1m
123	1.02m
Monkey	.980m
Dragon	.968m

https://www.forbes.com/sites/kateoflahertyuk/2019/04/21/these-are-the-worlds-most-hacked-passwords-is-yours-on-the-list/#2afa28f1289c

More top passwords

Names:	
Ashley	432,276
michael	425,291
daniel	368,227
jessica	324,125
charlie	308,939

Musicians:	
blink182	285,706
50cent	191,153
eminem	167,983
metallica	140,841
slipknot	140,833

Football teams:	
liverpool	280,723
chelsea	216,677
arsenal	179,095
manutd	59,440
everton	46,619

Fictional characters:	
superman	333,139
naruto	242,749
tigger	237,290
pokemon	226,947
batman	203,116

https://www.forbes.com/sites/kateoflahertyuk/2019/04/21/these-are-the-worlds-most-hacked-passwords-is-yours-on-the-list/#2afa28f1289c

So What Can We Do

Make the passwords harder for the computer to guess!

Intel’s rules

- The password must be at least 8 characters long.
- The password **must** contain at least:
    - one alpha character [a-zA-Z];
    - one numeric character [0-9];
    - one special character from this set:
      ` ! @ $ % ^ & * ( ) - _ = + [ ] ; : ' " , < . > / ?
- The password **must not**:
    - contain spaces;
    - begin with an exclamation [!] or a question mark [?];
    - contain your login ID.
- The first 3 characters cannot be the same.
- The sequence of the first 3 characters cannot be in your login ID.
- The first 8 characters cannot be the same as in your previous password.
- Passwords are treated as case sensitive.

Dartmouth

- It should be eight characters long using only numbers and upper- and lower-case letters. **Note**: Passwords longer than eight characters will not work to authenticate you with some applications used at Dartmouth, such as Kerberos and Oracle Calendar.
- There can be no more than four characters in sequence (e.g., **12345** or **abcde** are not allowed).
- It must contain at least five different characters (e.g., **2a3a2a3a** only contains three different characters so is not allowed).
- It cannot be a word found in the dictionary, including foreign languages (e.g., **password**).
- It cannot be a reversal of a word found in the dictionary (e.g., **drowssap**).
- It cannot be a word found in the dictionary, plus one additional character either before or after the word (e.g., **xalgebra** or **algebrax**).
- It cannot be a word found in the dictionary with numbers substituted for look-alike letters (e.g., **passw0rd** or **pa55word**).
- It cannot be a word found in the dictionary minus any punctuation, symbols, or numbers (e.g., **oclock** or **soninlaw**).

JP Morgan Chase - Dec 2019

- Must be 8-32 characters long
- Must include at least two of the following elements:
  - At least one letter (upper or lowercase)
  - At least one number
  - At least one special character from the following: # $ % ‘ ^ , ( ) * + . : | = ? @ /] [_ ` { } \ ! ; – ~
- Must be different than your previous five Passwords
- Must not match your User ID
- Must not include more than 2 identical characters (for example: 111 or aaa)
- Must not include more than 2 consecutive characters (for example: 123 or abc)
- Must not use the name of the financial institution (for example: JPM, MORGAN, CHASE)
- Must not be a commonly used password (for example: password1)

Bank of America - Dec 2019

- Contain 8 to 20 characters.
- Have at least 1 uppercase letter, 1 lowercase letter, and 1 number.
- Not repeat the same number or letter more than 3 times in a row.
- Not include spaces, and contain only the following special characters: @ # * ( ) + = { } / ? ~ ; , . - _

Wells Fargo - Dec 2019

Your password:
– Must be 6 to 14 characters.
– Must contain at least one letter and one number.
– May not contain nine or more numbers.
– May not be identical to your Username.
– May not repeat the same number or letter more than 3 times in a row.
– May not contain more than 3 sequential numbers or letters (such as ‘1234’ or ‘abcd’) in a row.
– May contain special characters (such as @, %, &, #).

Citigroup - Dec 2019

- The length of the Password must be from 6 characters to 50 characters.
- The characters must be alphanumeric (i.e. only letters from the English alphabet and numbers).
- The Password must contain at least one upper case letter, at least one lower case letter, and at least one number.
- The Password is case sensitive - Abc001 is **NOT** the same Password as abC001.
- It must not be the same as any of your account or card numbers, or your User ID.
- The Password must not contain 3 identical characters such as AAA, 3 sequential digits such as 123 or 321, 3 sequential letters such as Abc or cbA.
- The Password must not be the same as the User ID.

We recommend that you regularly change your Password.

Mitsubishi UFJ - Dec 2019

The new password can be between 8 to 32 alphanumeric characters in length.
Spaces are not allowed in your password.
Capital/small letters to be distinguished each other.
The new password must be different from any of the last three passwords used.

Question: how do they save the three previous passwords…?

“Eye-of-newt” password rules

Fillet of a fenny snake,
In the cauldron boil and bake;
Eye of newt and toe of frog,
Wool of bat and tongue of dog,
Adder's fork and blind-worm's sting,
Lizard's leg and howlet's wing,
For a charm of powerful trouble,
Like a hell-broth boil and bubble.

-- Macbeth, Act 1, Scene 1

Use a different password for each account

If the attackers get one of your passwords, they will try it elsewhere, and that usually works

Change Your Password Frequently

Because that’s what we do with crypto machines

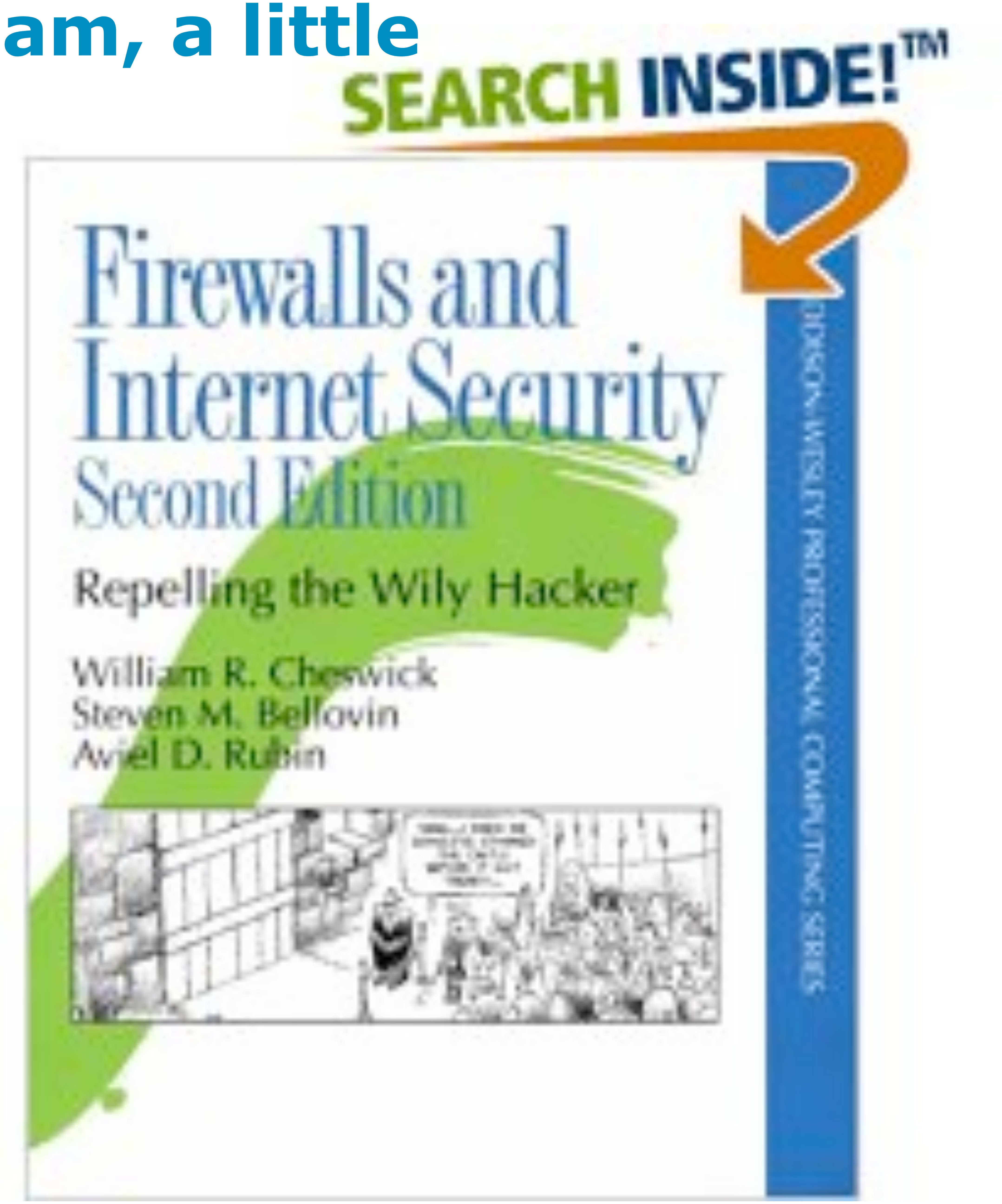
Don’t Reuse Passwords

Don’t Write Your Password Down

This is a usability nightmare! Eye-of-newt passwords are easy to test, and hard to type and remember

Who’s responsible for this?

Well, I am, a little



SEARCH INSIDE!™

Firewalls and Internet Security

Second Edition

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Results

- People violate many of these rules routinely, for usability reasons
- Stringent rules increase use of fall-back systems, which are usually less secure, or more expensive
- The rules don't make most things more secure in the face of most current threats

A note on Grandma

- **Helped Seaborg and Oppenheimer discover new elements**
- **Disk controller code for the Univac I**
- ***She was no dummy!***

THE MENTOR PROJECT®

https://mentorproject.org

None of these are grandma’s fault!

- ***Users are Not the Enemy*, A. Adams and M.A. Sasse, *Commun. ACM*, 42(12), 1999.**

It is simply poor engineering to expect people to select and remember passwords that are resistant to dictionary attacks

Can we do better?

Oh, yes!

100 Most Influential People in IT
eWeek, 2008-04-04

96. Dave Winer
Software developer and entrepreneur

Winer is the developer of RSS.

97. Thornton May
Florida Community College, IT Leadership Academy
May is a noted technology futurist.

98. William
Cheswick
Lead member of technical staff, AT&T Labs

Cheswick continues to innovate in the area of communications research.

99. Chris Anderson
Author
Anderson, editor in chief of Wired, proffered the notion of the niche in his book, “The Long Tail: Why the Future of Business Is Selling Less of More.”

100. Ben Bernanke
Chairman, Federal Reserve Board
No one will have a bigger impact on the fate of the nation’s banks and financial services companies, interest rates, or access to credit.

The four factors of authentication

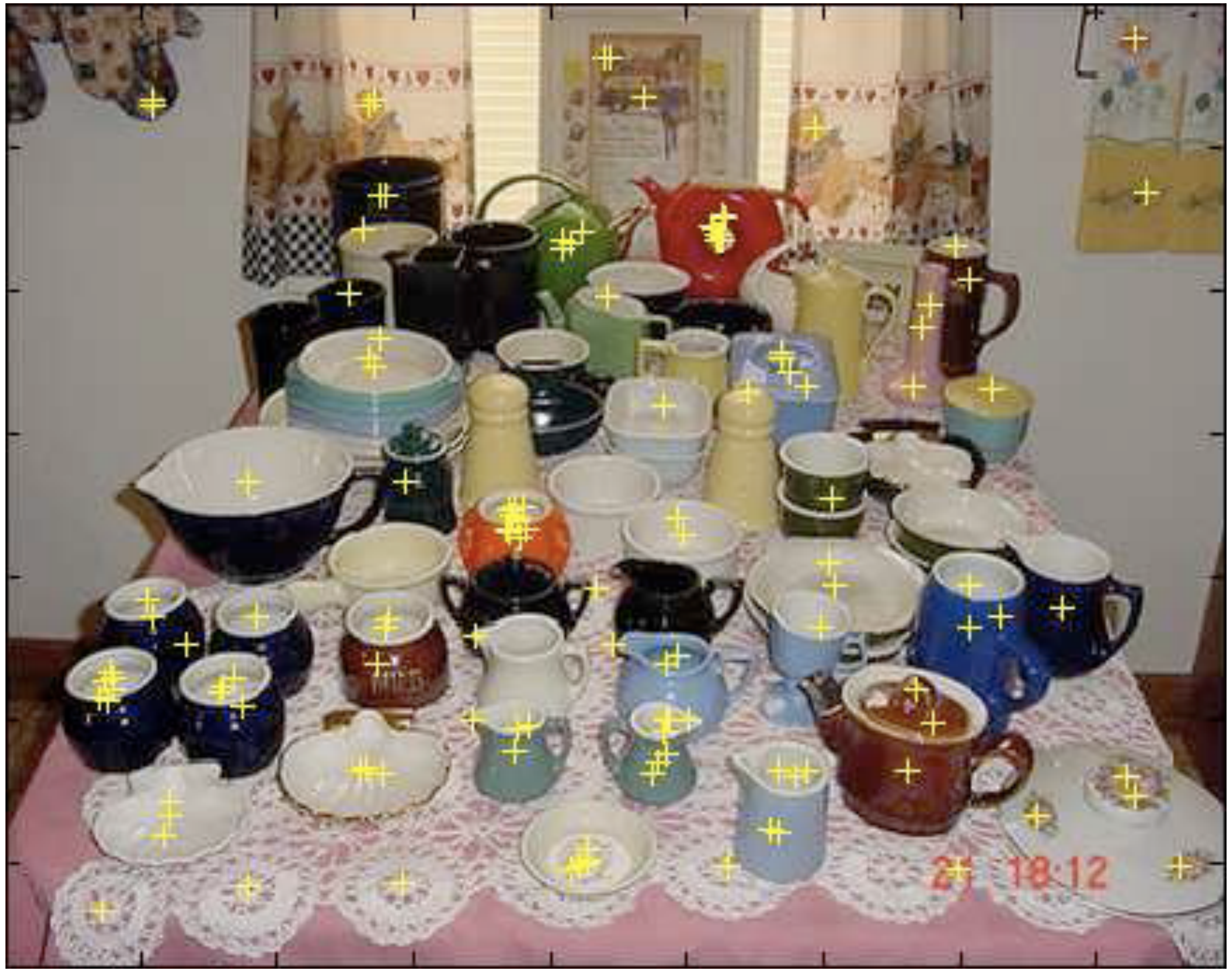
- Something you know
  - password, PIN, mother’s maiden name, etc
- Something you have
  - A key, electronic device, implant
- Something you are
  - fingerprint, face, DNA, voice print
- Your location
  - GPS, close to the authenticator (sonar!), etc.

Some Password Ideas

From academia, and me

For a complete survey, see

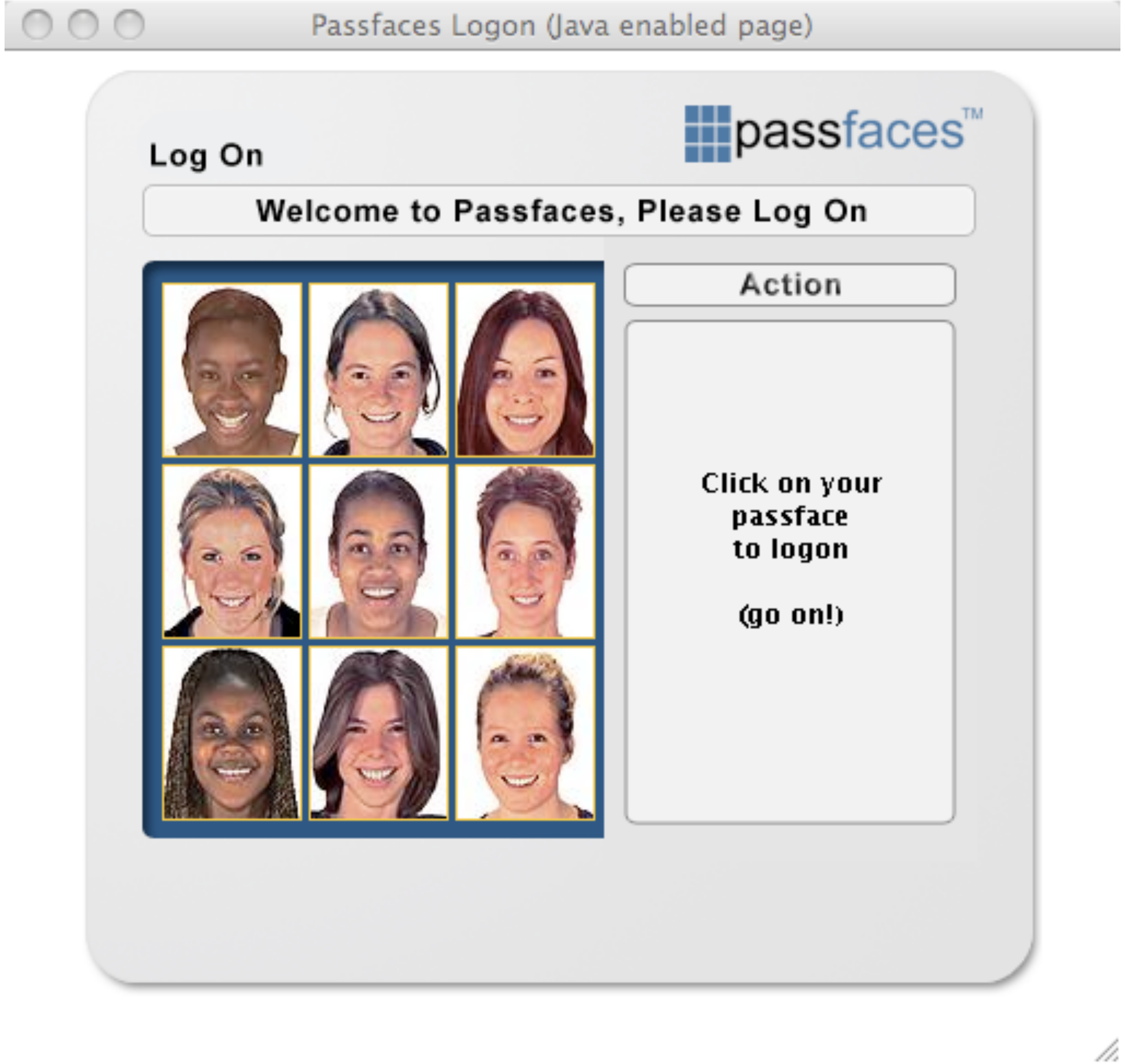
- http://people.scs.carleton.ca/~paulv/papers/gpsurvey-27sept2010.pdf



from *Dirik, Memon, Birget*; SOUPS 2007

of about 100

Passfaces



Passfaces Logon (Java enabled page)

passfaces™

Log On

Welcome to Passfaces, Please Log On

Action

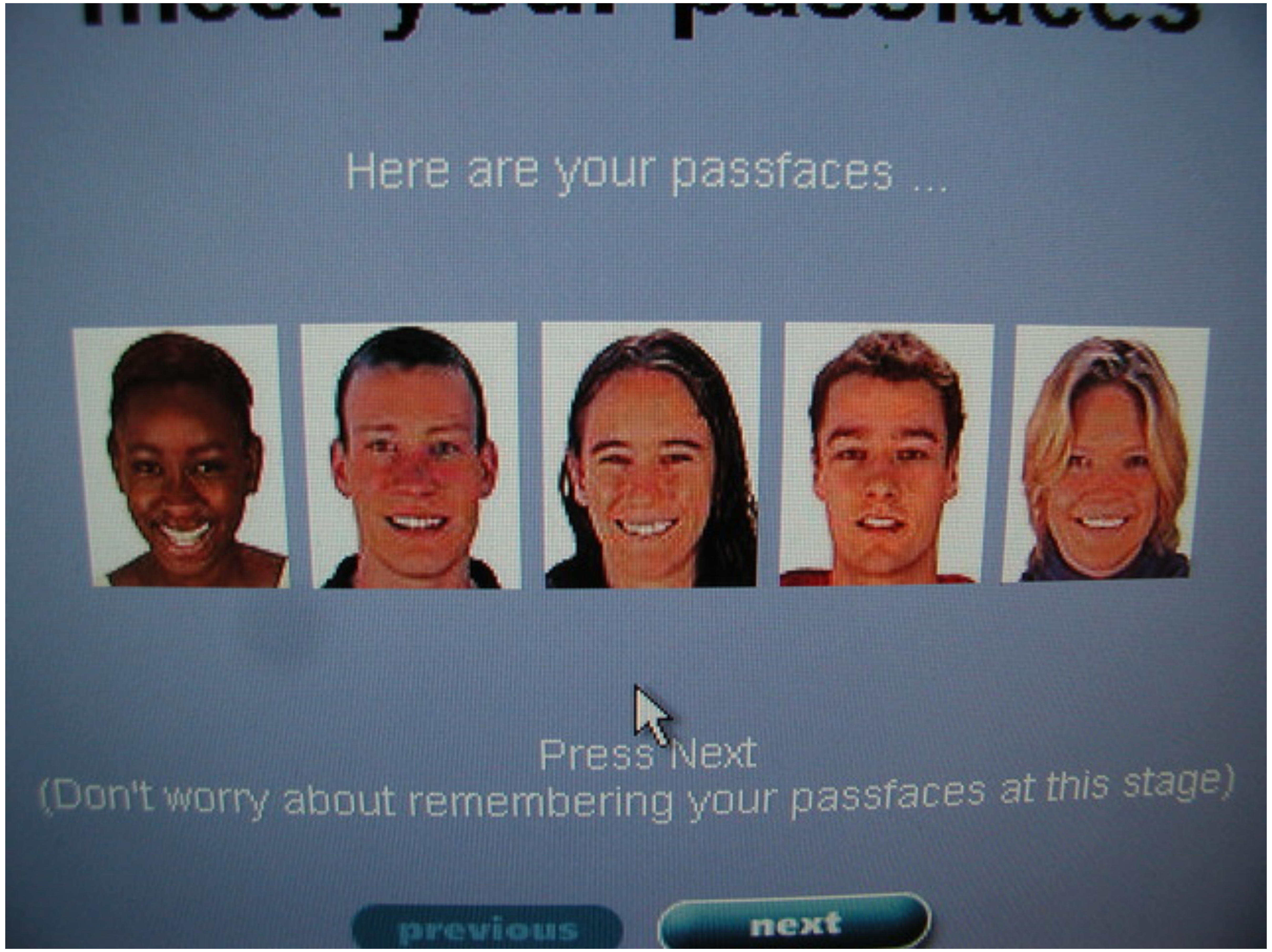
Click on your
passface
to logon

(go on!)

THE MENTOR PROJECT®

https://mentorproject.org

My passfaces

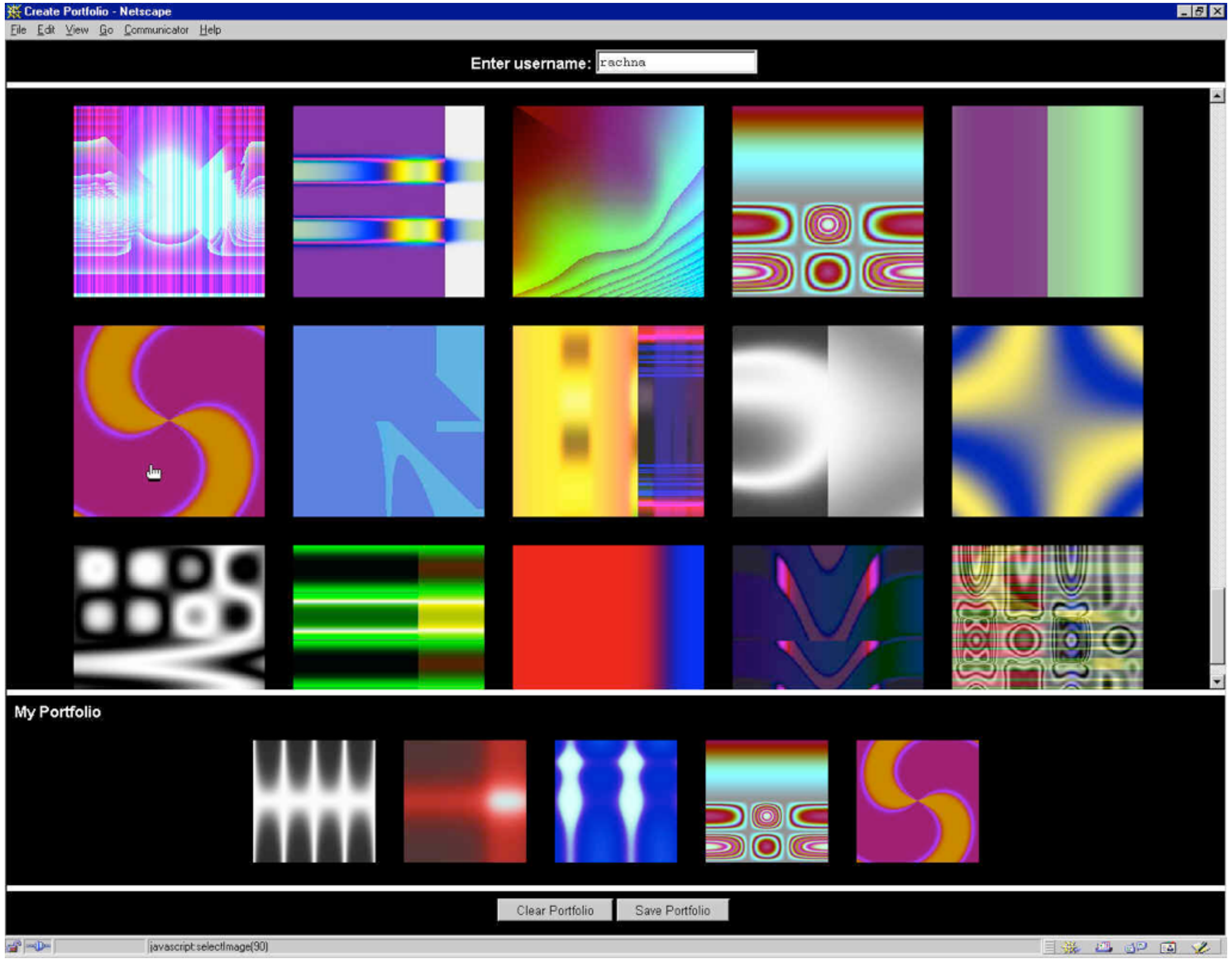


meet your passfaces

Here are your passfaces ...

Press Next
(Don't worry about remembering your passfaces at this stage)

Deja Vu (Recognition-based)



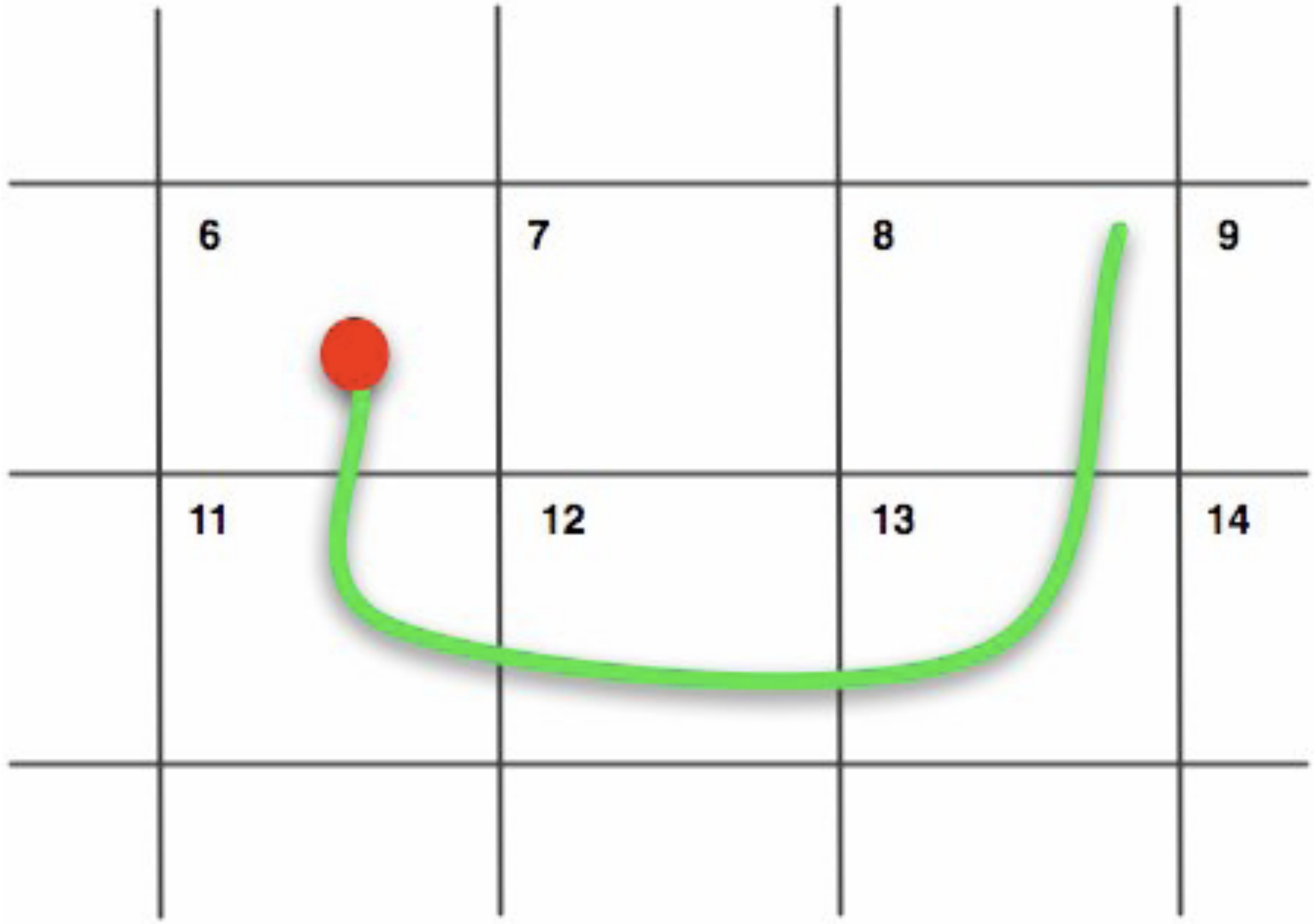
Create Portfolio - Netscape
File Edit View Go Communicator Help
My Portfolio
Clear Portfolio
Save Portfolio

Enter username: rachna

javascript:selectImage(90)

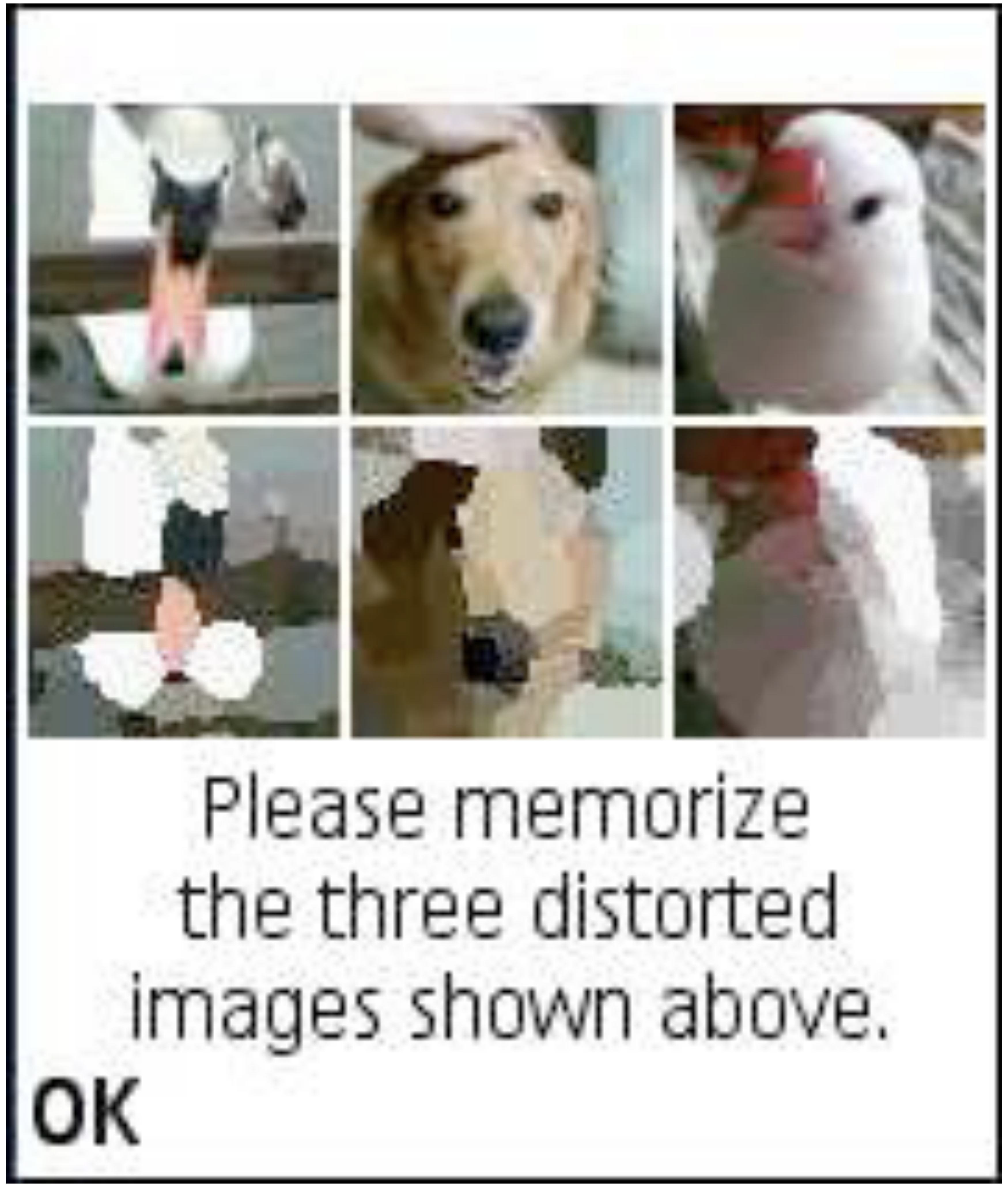
https://mentorproject.org

Draw a Secret

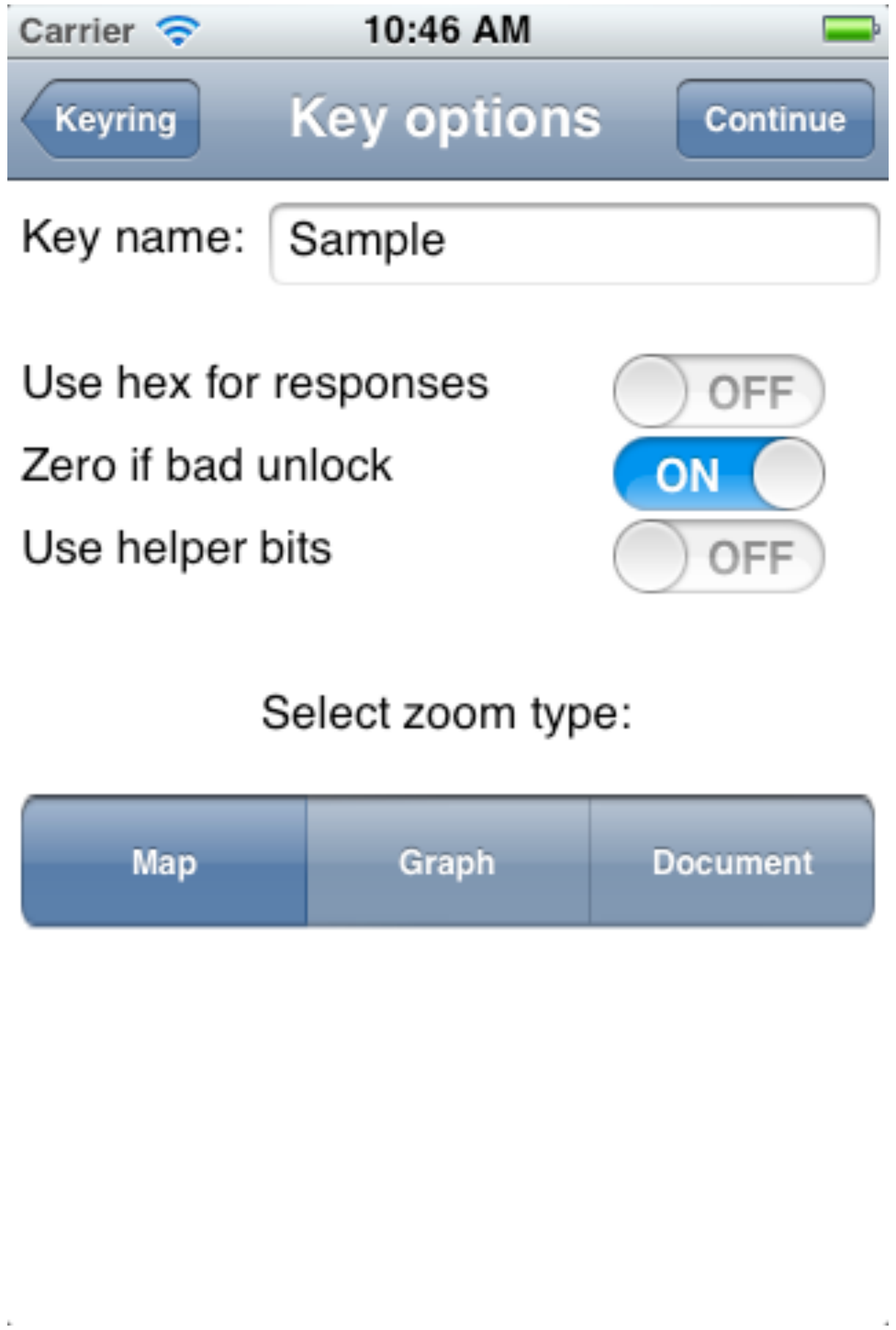


Lin, Dunphy, *et al.* SOUPS 2007

Use Your Illusion (SOUPS 2008)



Please memorize the three distorted images shown above.



Key options

Key name: Sample

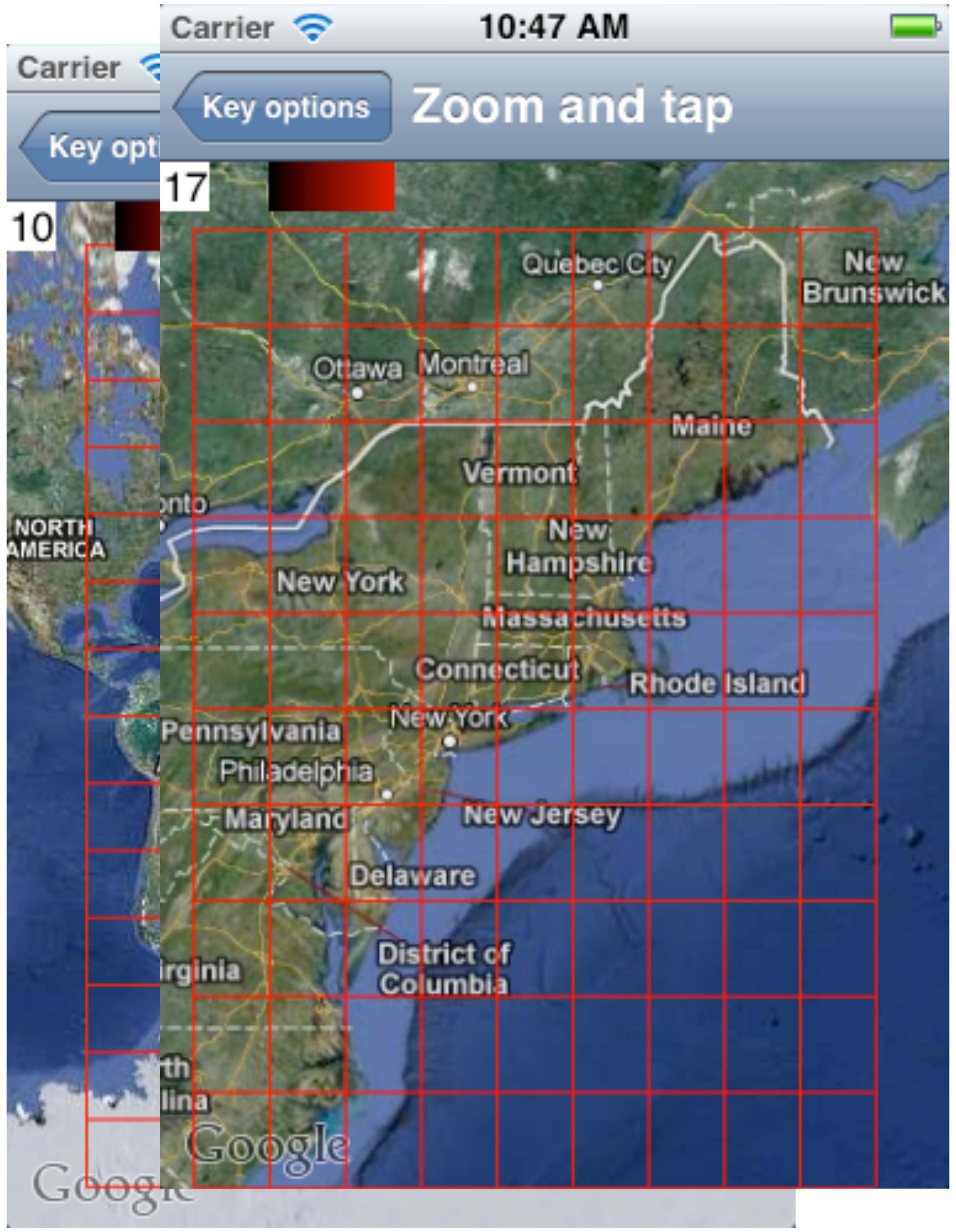
Use hex for responses OFF

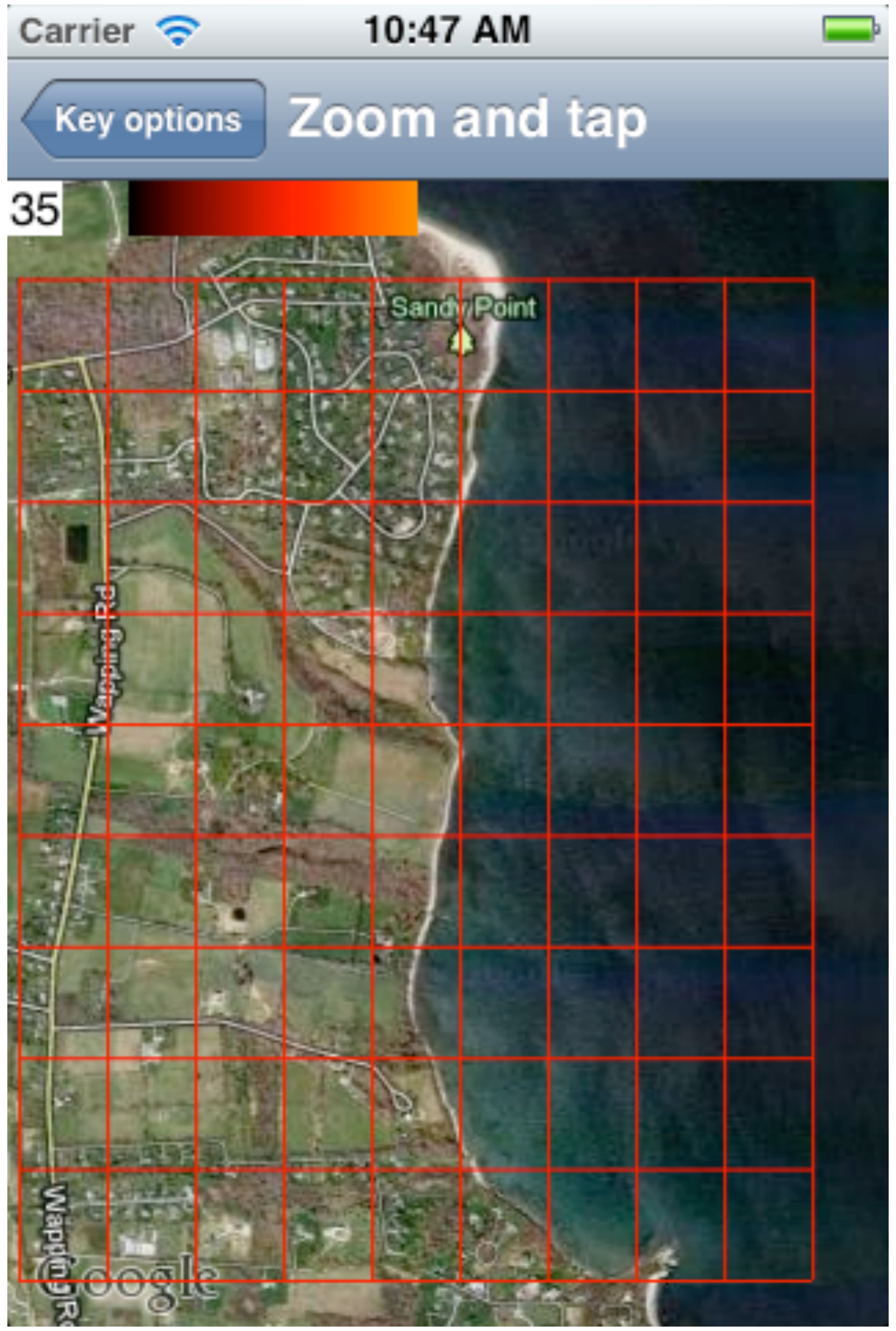
Zero if bad unlock ON

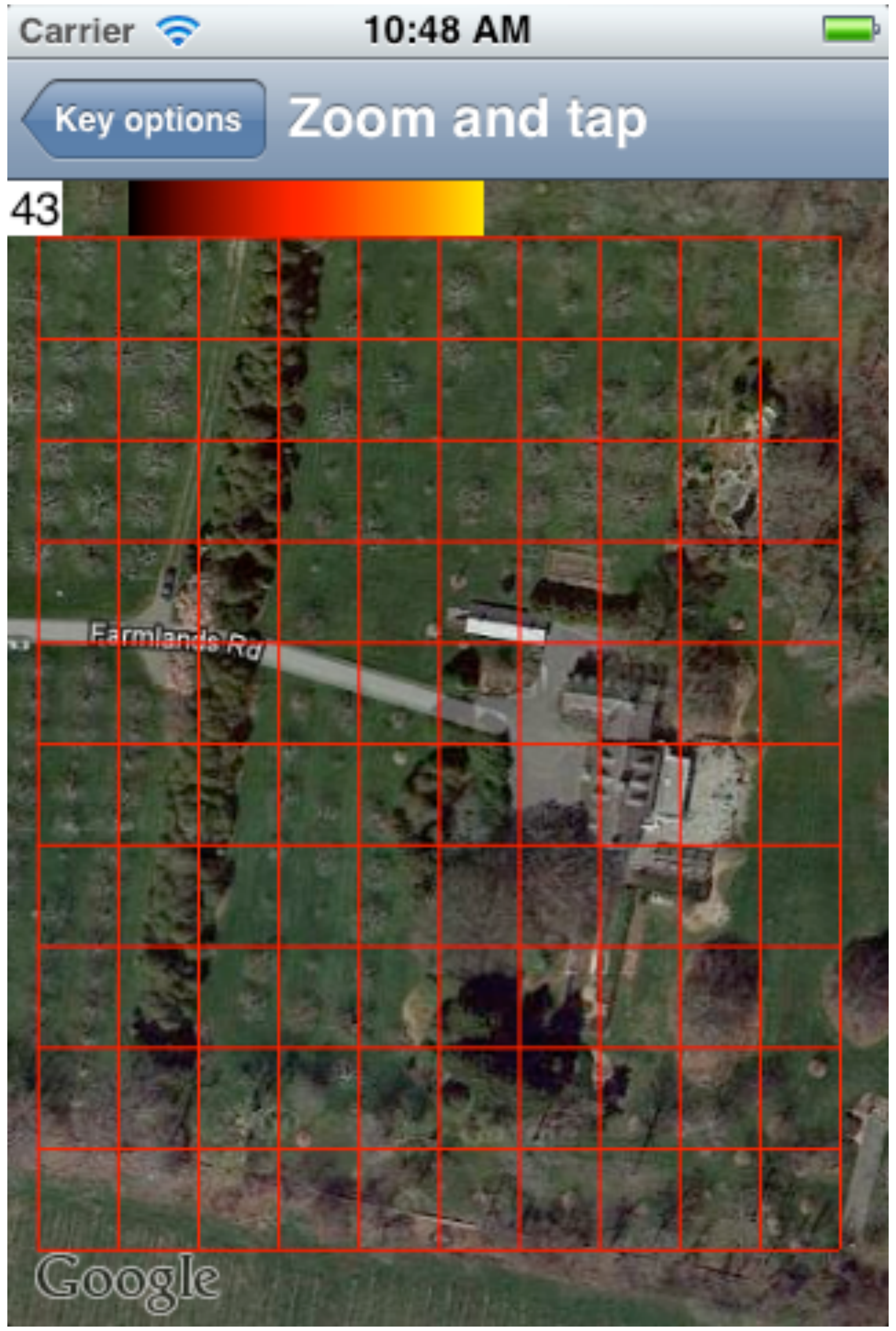
Use helper bits OFF

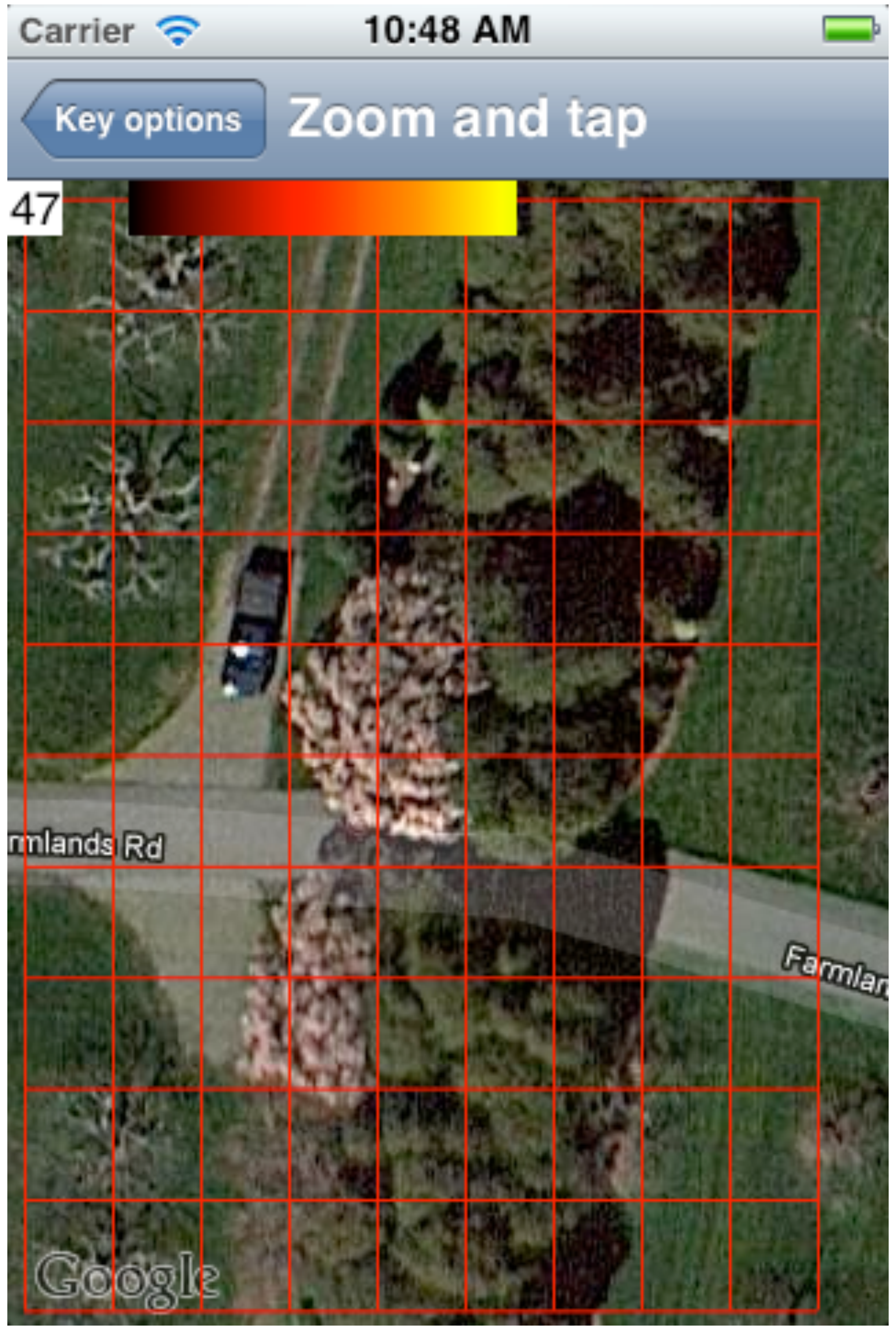
Select zoom type:

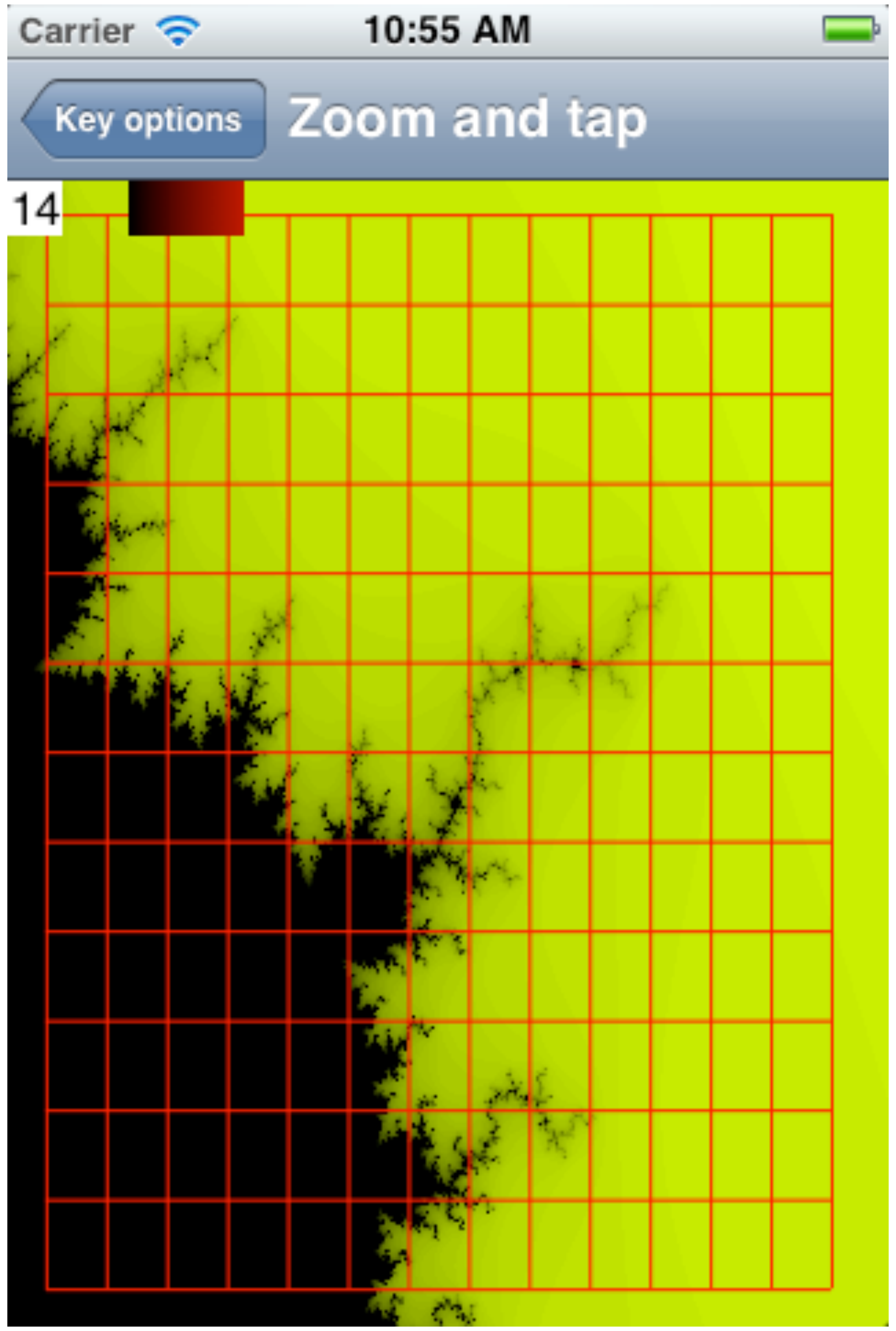
Map | Graph | Document



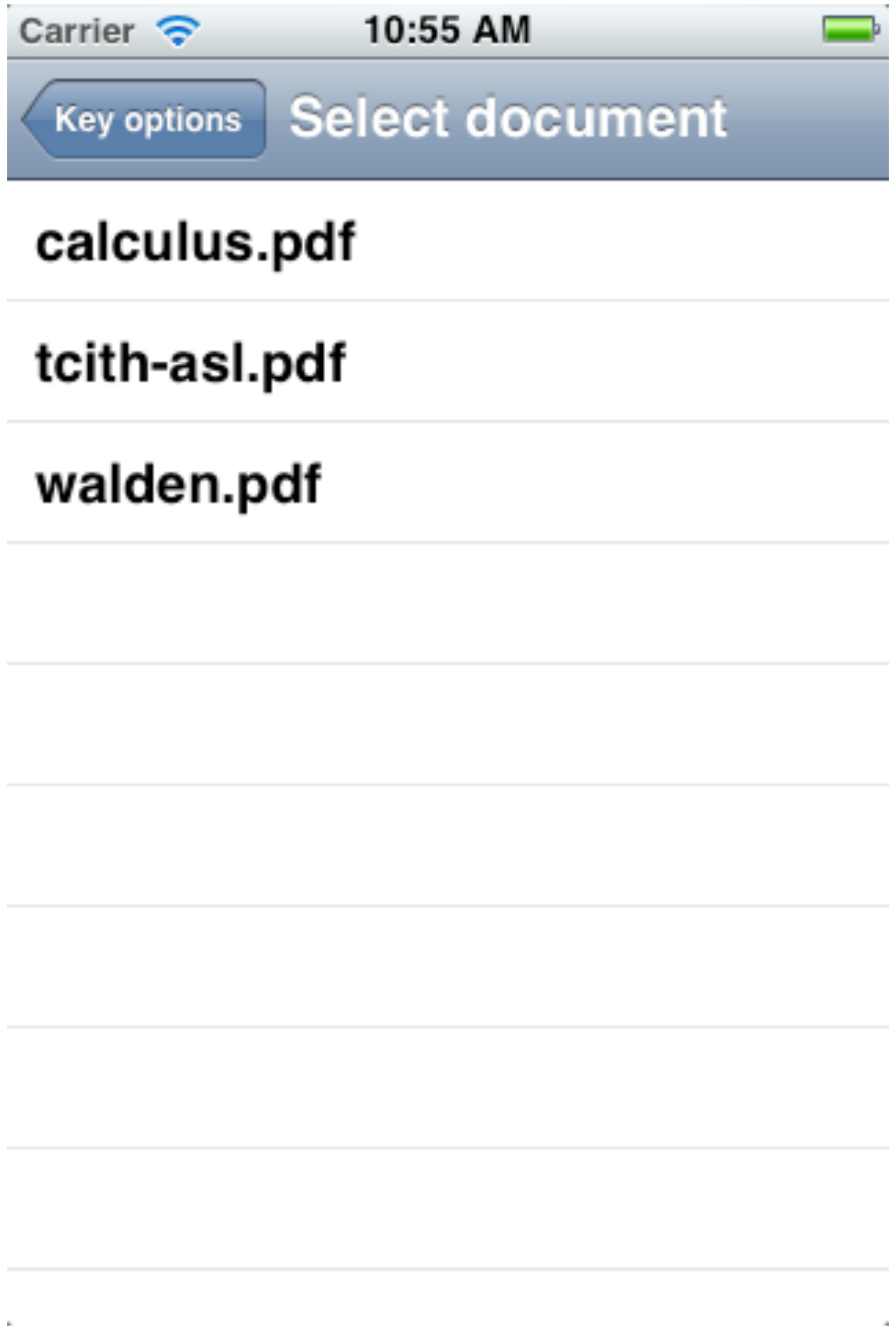

Carrier
10:47 AM
Key options
Zoom and tap
35
Sandy Point
Wapping Rd
Wapping Rd
Google


Carrier
10:48 AM
Key options
Zoom and tap
43
Farmlands Rd
Google


Carrier
10:48 AM
Key options
Zoom and tap
47
rmlands Rd
Farmlan
Google



Carrier
10:55 AM
Key options
Zoom and tap
14

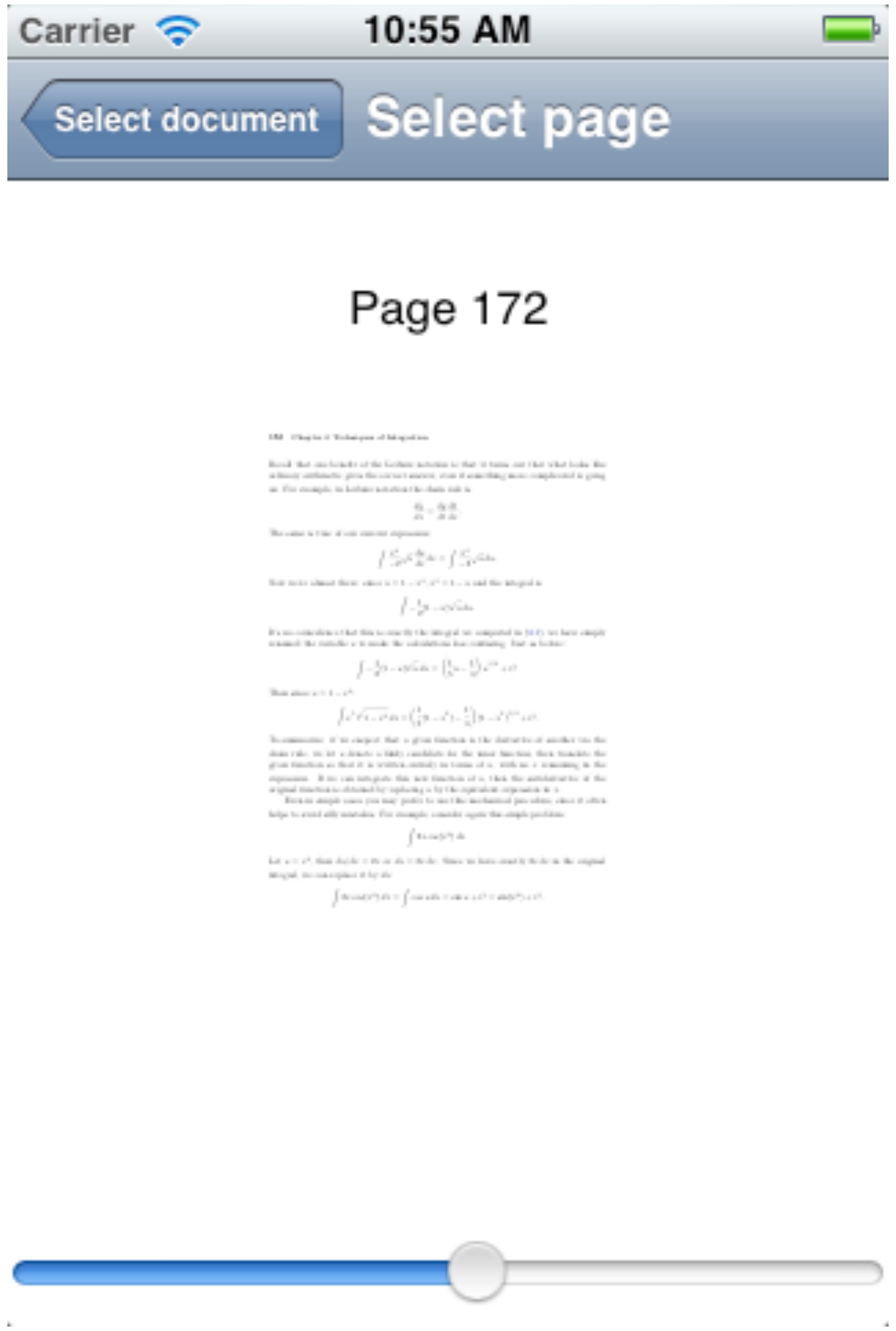


Select document

calculus.pdf

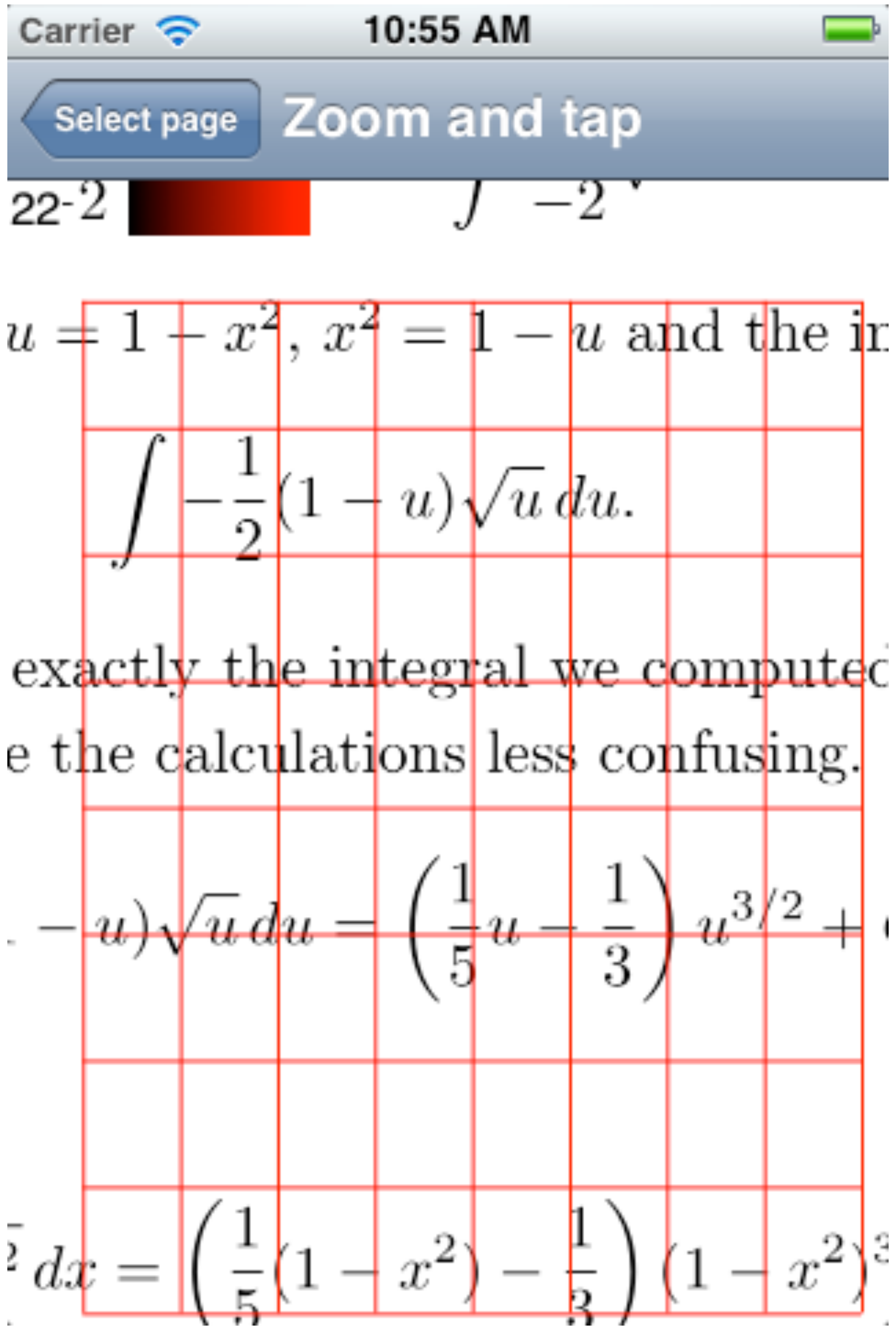
tcith-asl.pdf

walden.pdf



Select page

Page 172



Zoom and tap

$u = 1 - x^2$, $x^2 = 1 - u$ and the ir

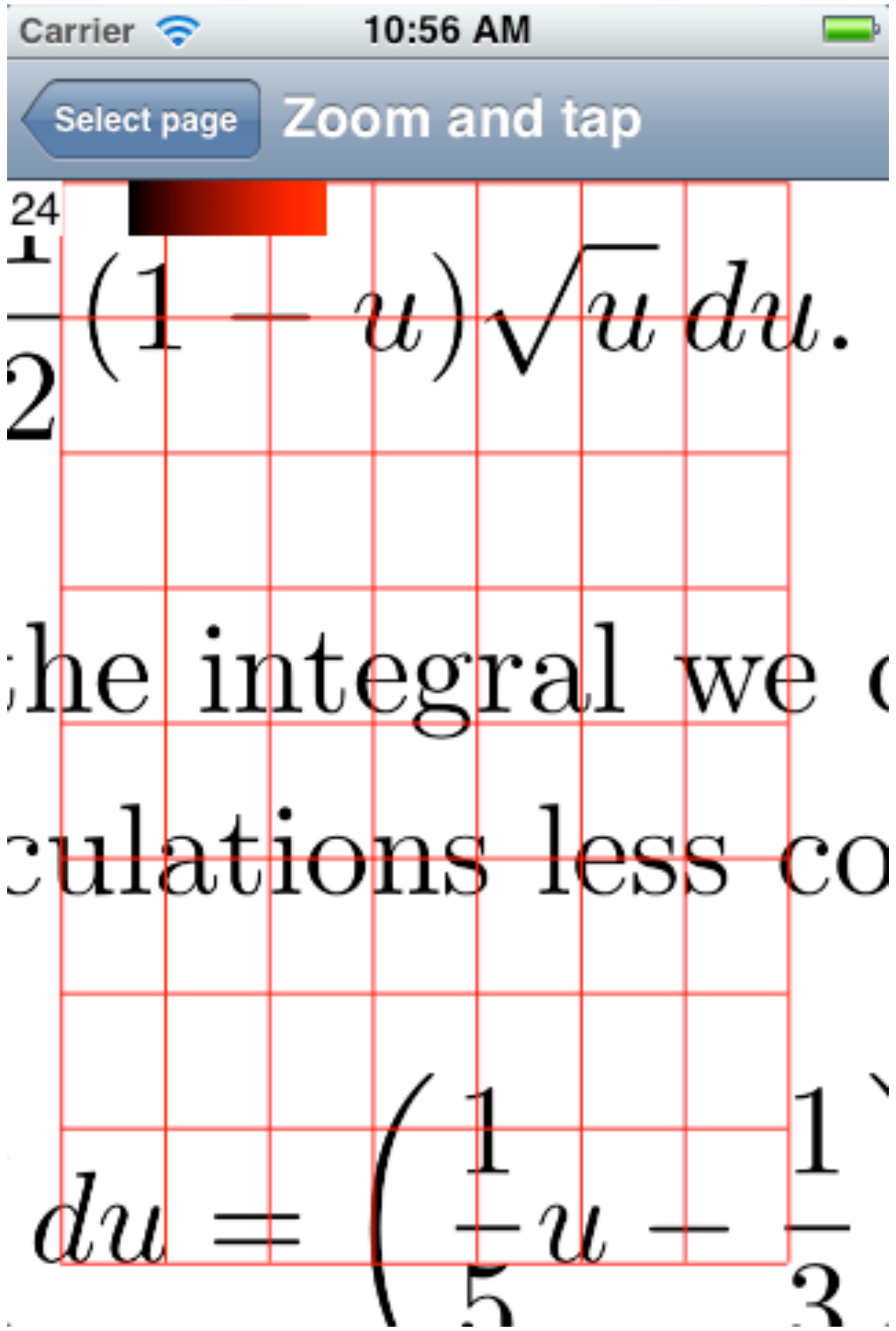
$$\int -\frac{1}{2}(1 - u)\sqrt{u}\,du.$$

exactly the integral we computec

e the calculations less confusing.

$$-u)\sqrt{u}\,du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} +$$

$$dx = \left(\frac{1}{5}(1 - x^2) - \frac{1}{3}\right)(1 - x^2)$$

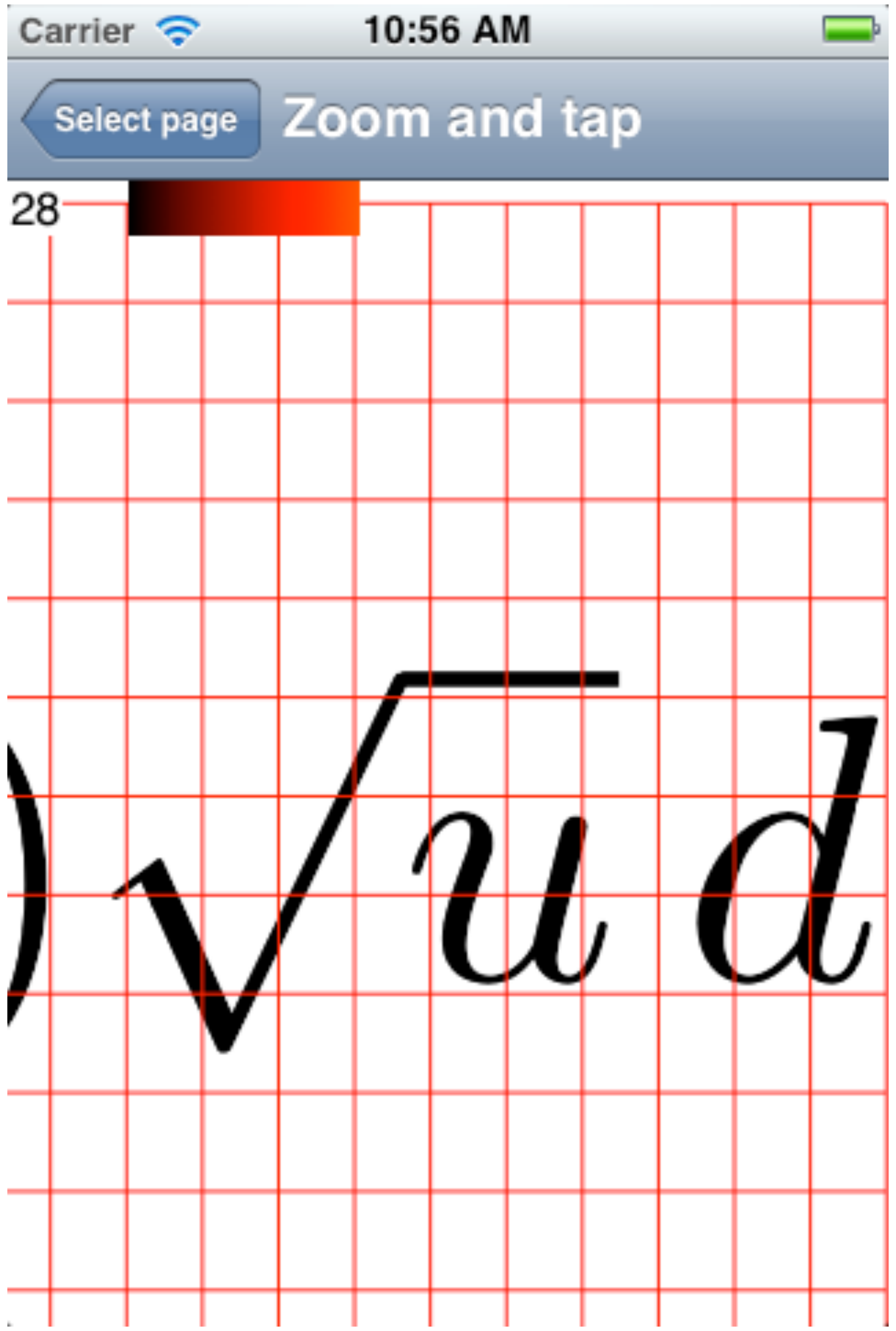


$\frac{1}{2}(1-u)\sqrt{u}\,du.$

he integral we

culations less co

$du = \Big(\frac{1}{5}u - \frac{1}{3}$



$)\sqrt{u}\,d$

Problem

- **One-time passwords solve a lot of password problems**
- **One-time passwords (usually challenge/response) require something you have**
- **Equipment can be expensive, and it may be necessary to authenticate when equipment is not available**

34

210
NIA INSURANC

NIA INSURA

Baseball players

- Under a lot of stress
- Information is often vital to the game
- Not always the sharpest knife in the drawer
  - Babe Ruth forgot the signs five steps out on the field

Key insight?

- Humans can’t compute well, but perhaps they can obfuscate well enough

Proposed approach

- **Use human-computed responses to computer challenges for authentication**
- **Though the computation is easy, much of the challenge and response is ignored**
- **Obfuscation and lack of samples complicate the attacker's job beyond utility**

```
Challenge:                             Response:

ches 00319 Thu Dec 20 15:32:22 2001    23456bcd;f.k
root 00294 Fri Dec 21 16:47:39 2001    nj3kdi2jh3yd6fh:/
ches 00311 Fri Dec 21 16:48:50 2001    /ldh3g7fgl
ches 00360 Thu Jan 3 12:52:29 2002     jdi38kfj934hdy;dkf7
ches 00416 Fri Jan 4 09:02:02 2002     jf/l3kf.l2cxn. y
ches 00301 Fri Jan 4 13:29:12 2002     j2mdjudurut2jdnch2hdtg3kdjf;s’/s
ches 00301 Fri Jan 4 13:29:30 2002     j2mdgfj./m3hd’k4hfz
ches 00308 Tue Jan 8 09:35:26 2002     /l6k3jdq,
ches 84588 Thu Jan 10 09:24:18 2002    jf010fk;.j
ches 84588 Thu Jan 10 09:24:35 2002    heu212jdg431j/
ches 00306 Thu Jan 17 10:46:00 2002    jfg.bv,vj/,1
ches 00309 Fri Jan 18 09:37:09 2002    no way 1 way is best!/1
ches 00309 Fri Jan 18 09:37:36 2002    jzw                          * no *
ches 00368 Tue Jan 22 09:51:41 2002    84137405jgf/
ches 77074 Tue Feb 19 09:02:52 2002    d                            * no *
ches 77074 Tue Feb 19 09:02:57 2002    hbcg3]’d/
ches 00163 Mon Feb 25 09:24:30 2002    d                            * no *
ches 00163 Mon Feb 25 09:24:35 2002    ozhdkf0ey2k/.,vk0l
ches 00156 Tue Mar 12 12:41:12 2002    3+4=7 but not 10 or 4/2
ches 00161 Fri Mar 15 09:41:20 2002    /.,kl9djfir
ches 00161 Fri Mar 15 09:41:36 2002    3                            * no *
ches 00160 Mon Mar 25 08:52:59 2002    222
ches 00160 Mon Mar 25 08:53:09 2002    2272645
ches 29709 Mon Apr 1 11:36:34 2002     4
ches 41424 Mon Apr 8 09:49:09 2002     ab3kdhf
ches 85039 Tue Apr 9 09:46:06 2002     04
ches 00161 Thu Apr 18 10:49:14 2002    898for/dklf7d
```

Pass-authentication

- Literature goes back to 1967
- A variety of names used: *reconstructed passwords, pass-algorithms, human-computer cryptography, HumanAut, secure human-computer identification, cognitive trapdoor games, human interactive proofs*

Possible uses

- emergency holographic logins (“passwords of last resort”)
- use from insecure terminals, when single session eavesdropping is probably not a problem
- if a solution is found: daily logins
- home run: online transactions: banking

Can Something You Know Be Saved?

Baris Coskun and Cormac Herley, in *Proc. 11th Information Security Conference (ISC 2008)*, pp. 421-440, Springer-Verlag [September 2008]

Can “something you know be saved?”

- I think so
- and, we don’t have a choice in most cases
- security and convenience: tradeoff?
- It is going to be one of the authentication factors
  - something you know
  - something you have
  - something you are
  - where you are
  - .....

We have much better solutions than eye-of-newt passwords

- **Limit guesses**
- **Lock the account (or at least slow down the tries)**
- **Multifactor authentication**
- **Authentication devices (“tokens”)**
- **Use your words**
- **Password vaults**

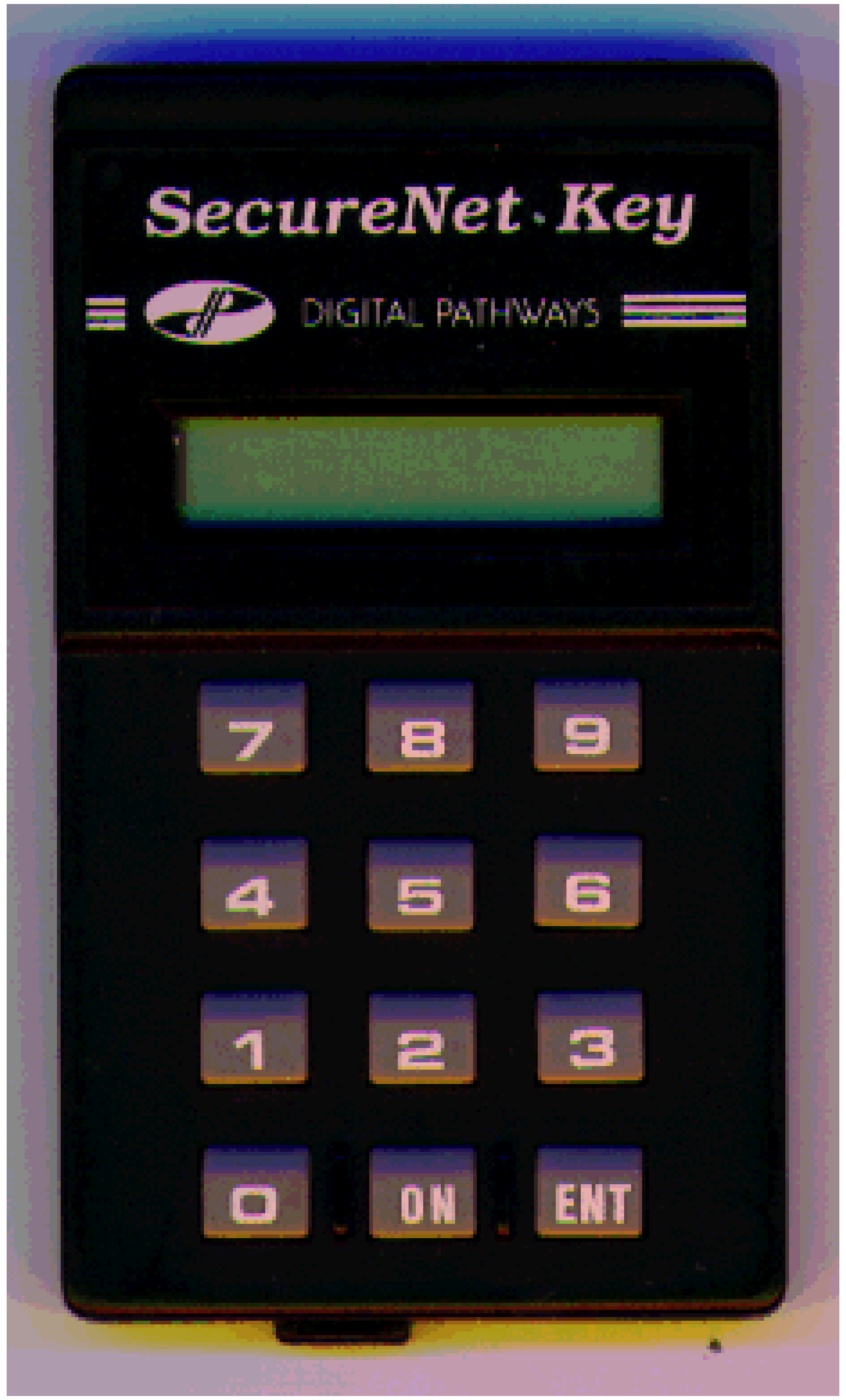
Multi-factor authentication

- Something you have, something you know, something you are
  - A device, a PIN or password, some biological traits
- Where you are
- Your phone number, and email account
  - Your email password is probably the most important authentication item you have.
- Properties of your phone connection
- Combinations of these are much harder to crack, even if individual tests are pretty weak

Authentication tokens

Getting out of the game

SecureNet Key SNK-004



A login from my distant past

```
RISC/os (inet)

Authentication Server.

Id? ches
Enter response code for 70202: 04432234


Destination? cetus
$
```

Challenge/Response passwords

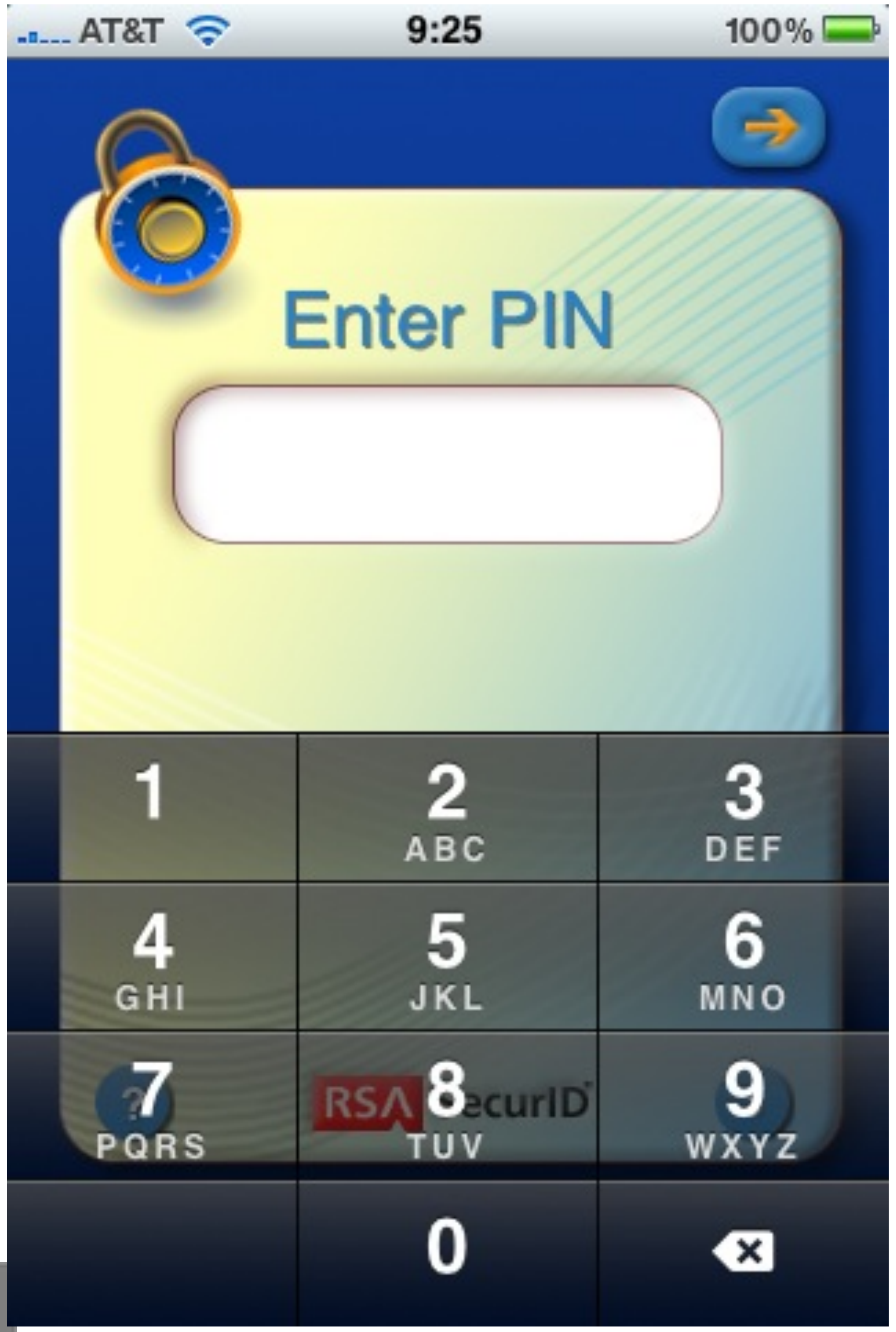
- Gets us out of the game
- Sniffing is not useful
- Man-in-the-middle can still be used
- Pretty much nothing to forget
- A PIN is helpful to make two-factor authentication
- Surprisingly cheap: $20 in 1989

SecureID

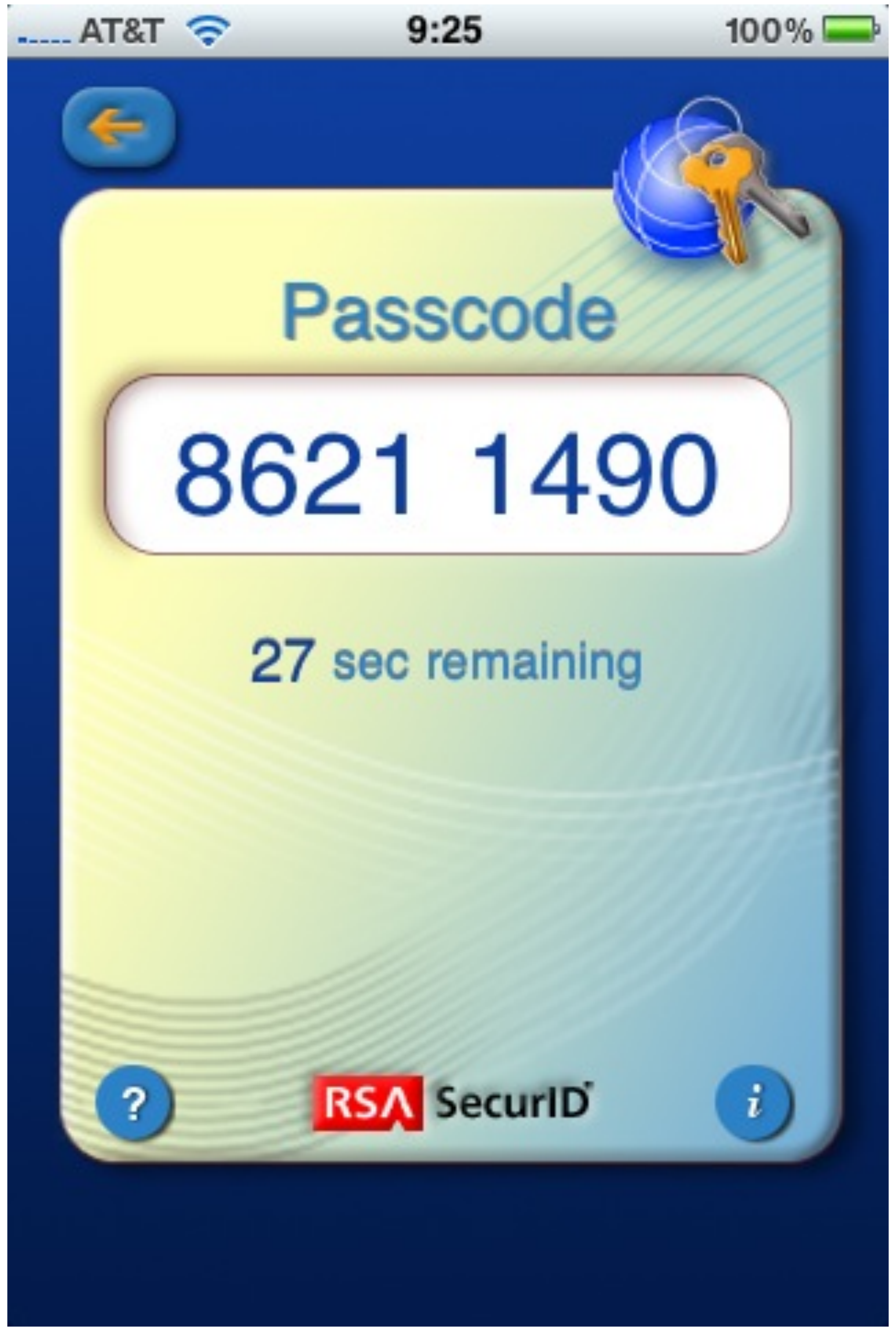
Why aren’t these ubiquitous?

- Cheap devices available before 1990
- People hate:
  - Having to carry the device
  - Entering the challenge (why SNK lost)
  - Entering the response
  - Carrying multiple devices
- *BUT*: You carry keys to use your car. Why not to authenticate on your computer?

RSA Softkey



Enter PIN



Passcode

8621 1490

27 sec remaining

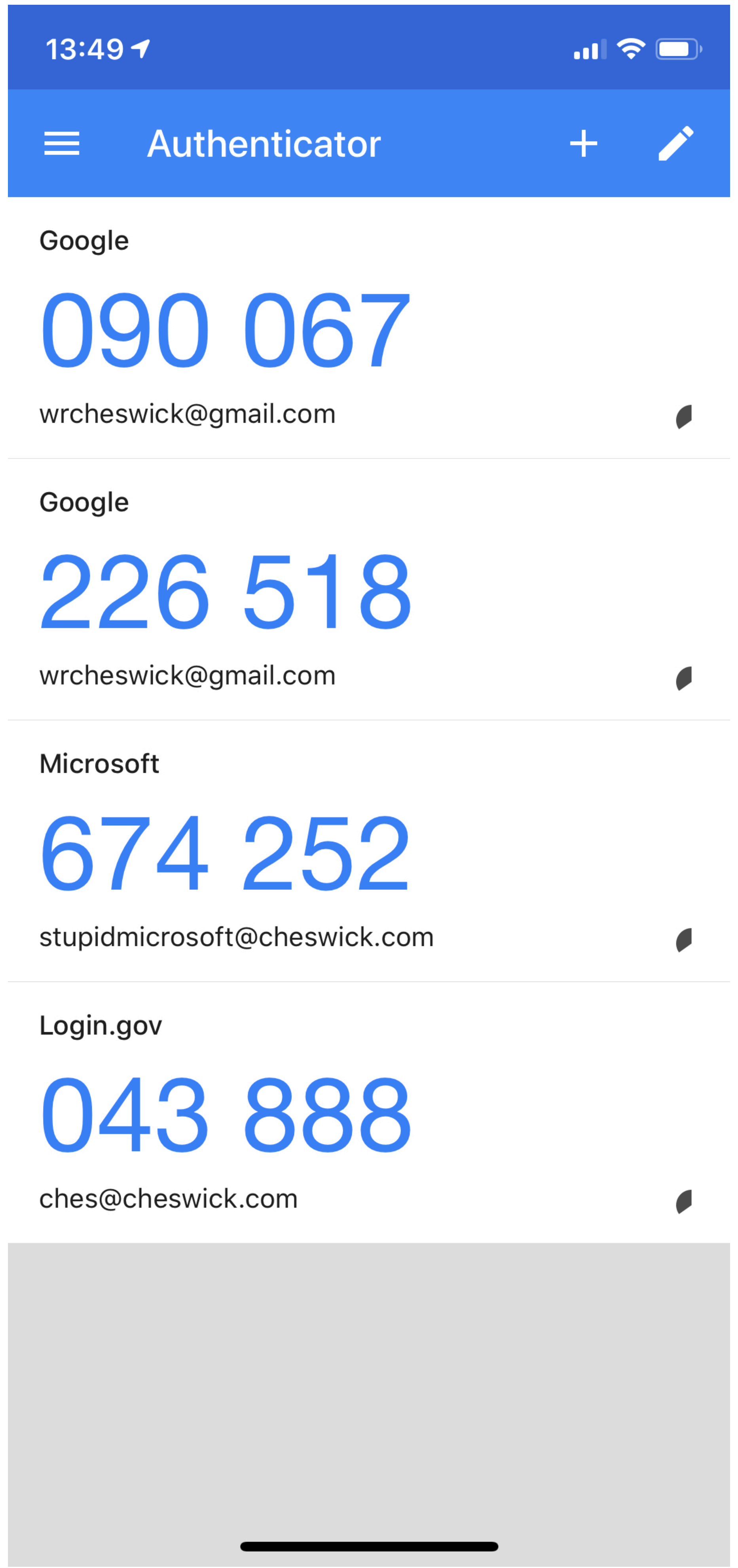
THE MENTOR PROJECT®

https://mentorproject.org

Great Things about the Softkey

- You always have your iPhone with you
- A bad PIN simply gives the wrong answer
- That means that the program doesn’t know the right answer
- That means that forensics can’t run a dictionary attack on it with having an observed login
- That means that a lost iPhone isn’t an authentication disaster

We have smart "phones" now, with good security



13:49

Authenticator

Google

090 067

wrcheswick@gmail.com

Google

226 518

wrcheswick@gmail.com

Microsoft

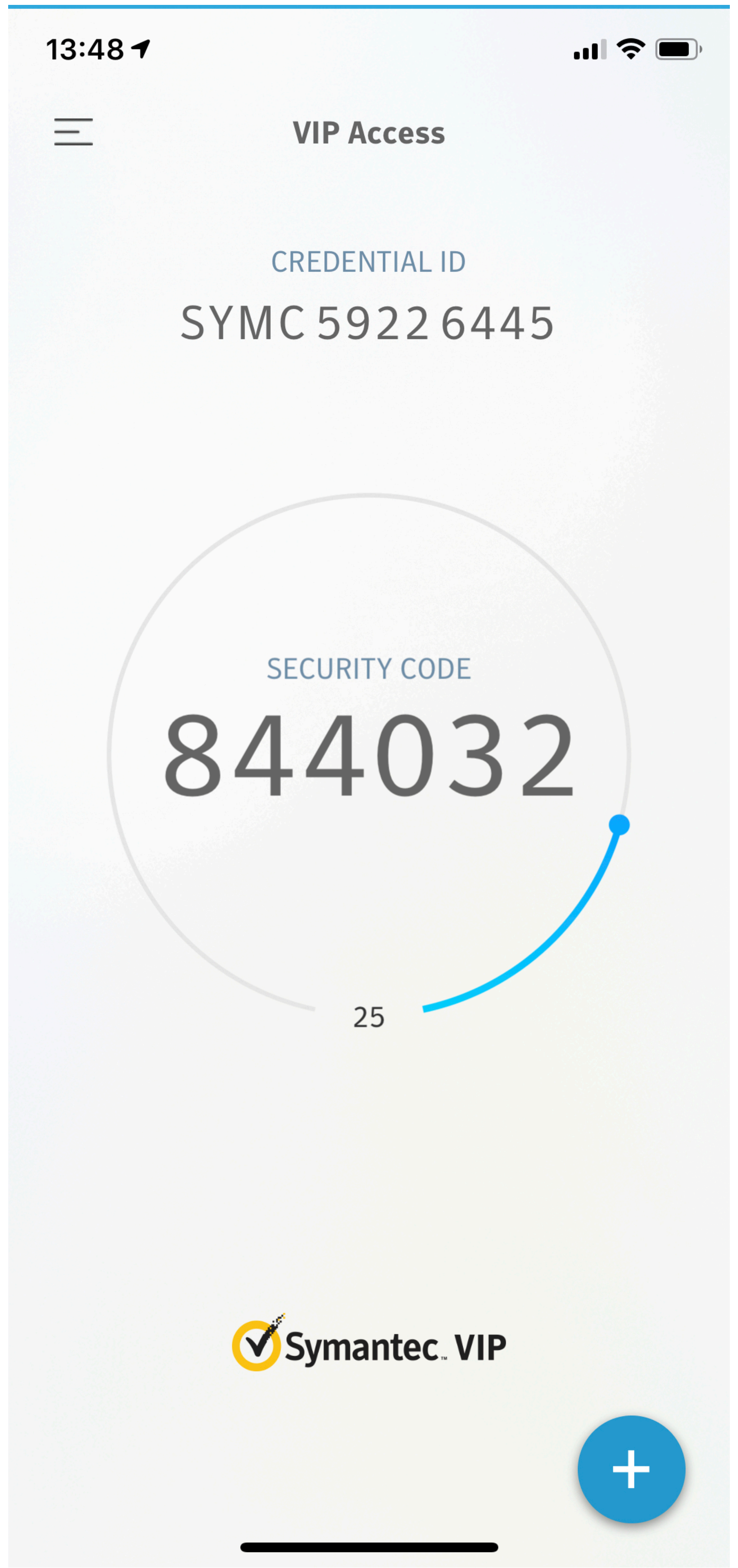
674 252

stupidmicrosoft@cheswick.com

Login.gov

043 888

ches@cheswick.com



13:48

VIP Access

CREDENTIAL ID

SYMC 5922 6445

SECURITY CODE

844032

25

Symantec. VIP

Suggestion: Less painful account locking

- Don’t count duplicate password attempts
  - they probably thought they mistyped it
- Make the password hint about the primary password, and don’t have a (weak) secondary
- Allow a trusted party to vouch for the user, so he can change his password
- Lock the account in increasing time increments
- Remind the user of password rules

Still Want Your Strong Passwords?
Grasping the “passphrase” nettle

Okay, fine. But let’s make them fun, or at least easier to type (and tap)

https://cheswick.com/insult

Insult passphrase generator

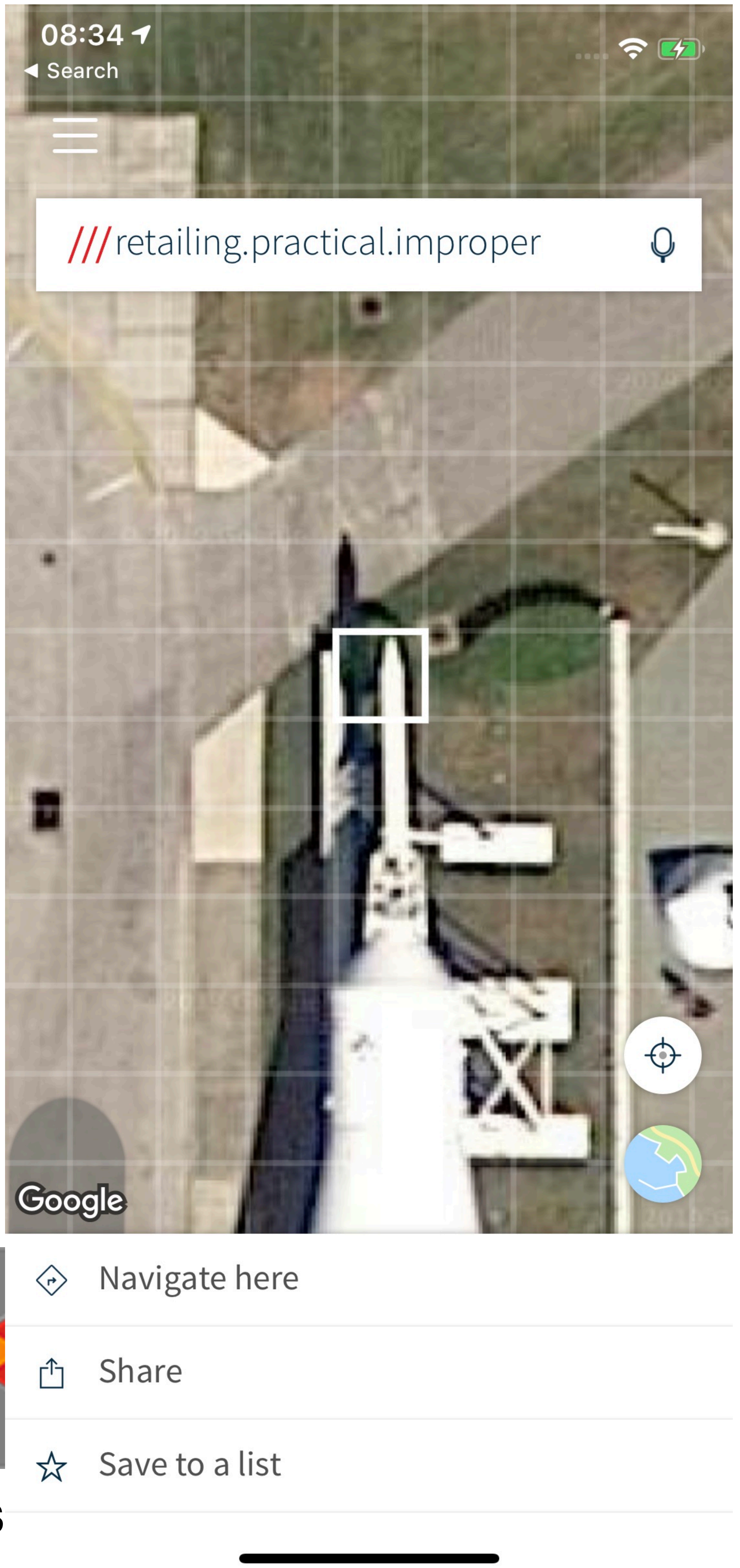
Insult code by Ron Hardin.

```
You unlikable barracks bag of tabid flying fish barf
You ugly mortar of incontinent guitarfish filings
You objectionable pottle of encephalitic Marco Polo's sheep dung
You ungraced filing box of unhygenic bluebottle offscourings
You uglified bundle of polluted tuna flatulence
You uncomely platter of dropsical cone-nose residue
You ill-featured soup bowl of diabetic tree frog egesta
You lamentable billy of virulent ibex exudation
You unpleasing pannier of ravaged butterfly agama settlings
You unattractive honeypot of miasmatic water buffalo extravasation
```

Work factor, ~42 bits, pretty good

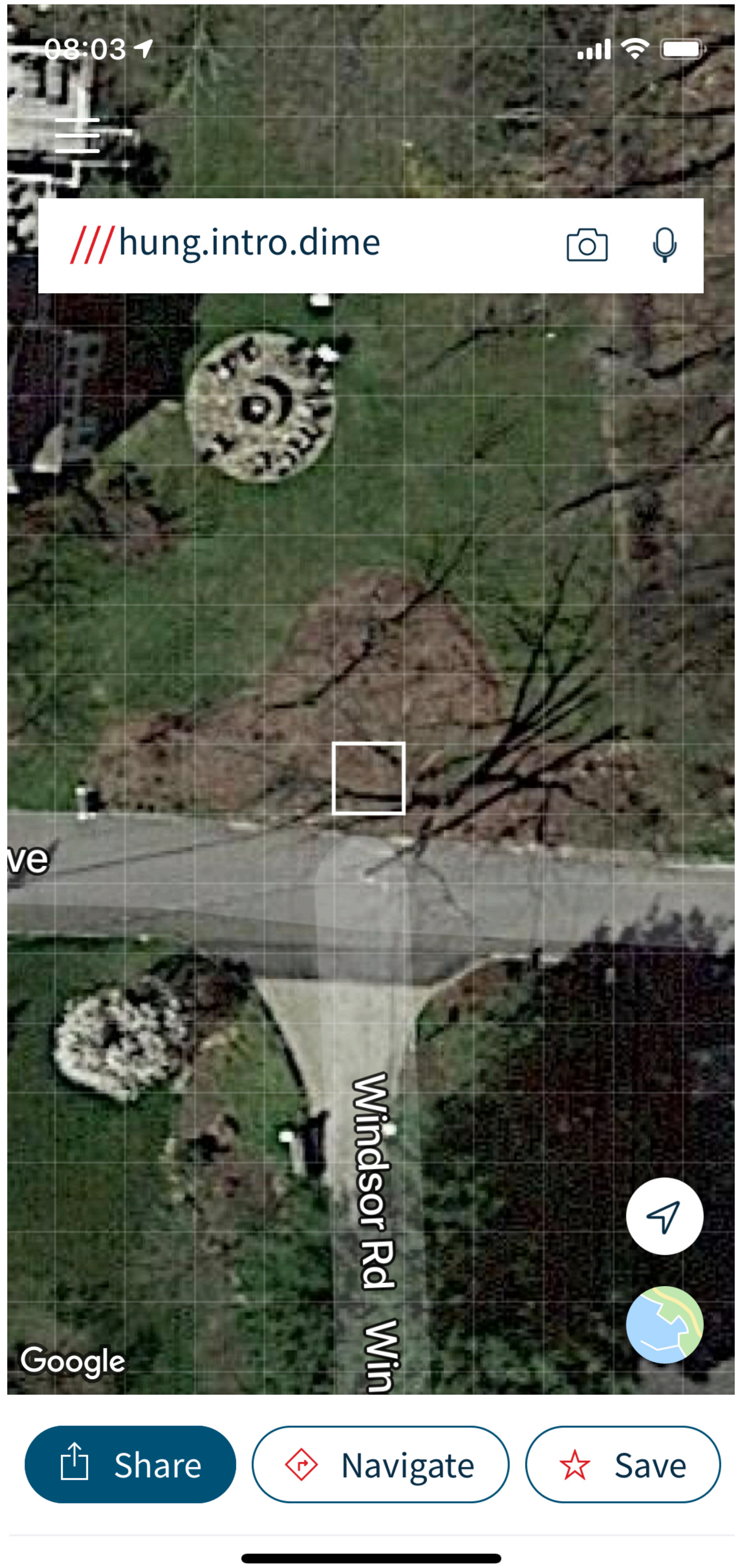
What three words:

Rocket garden at Cape Canaveral



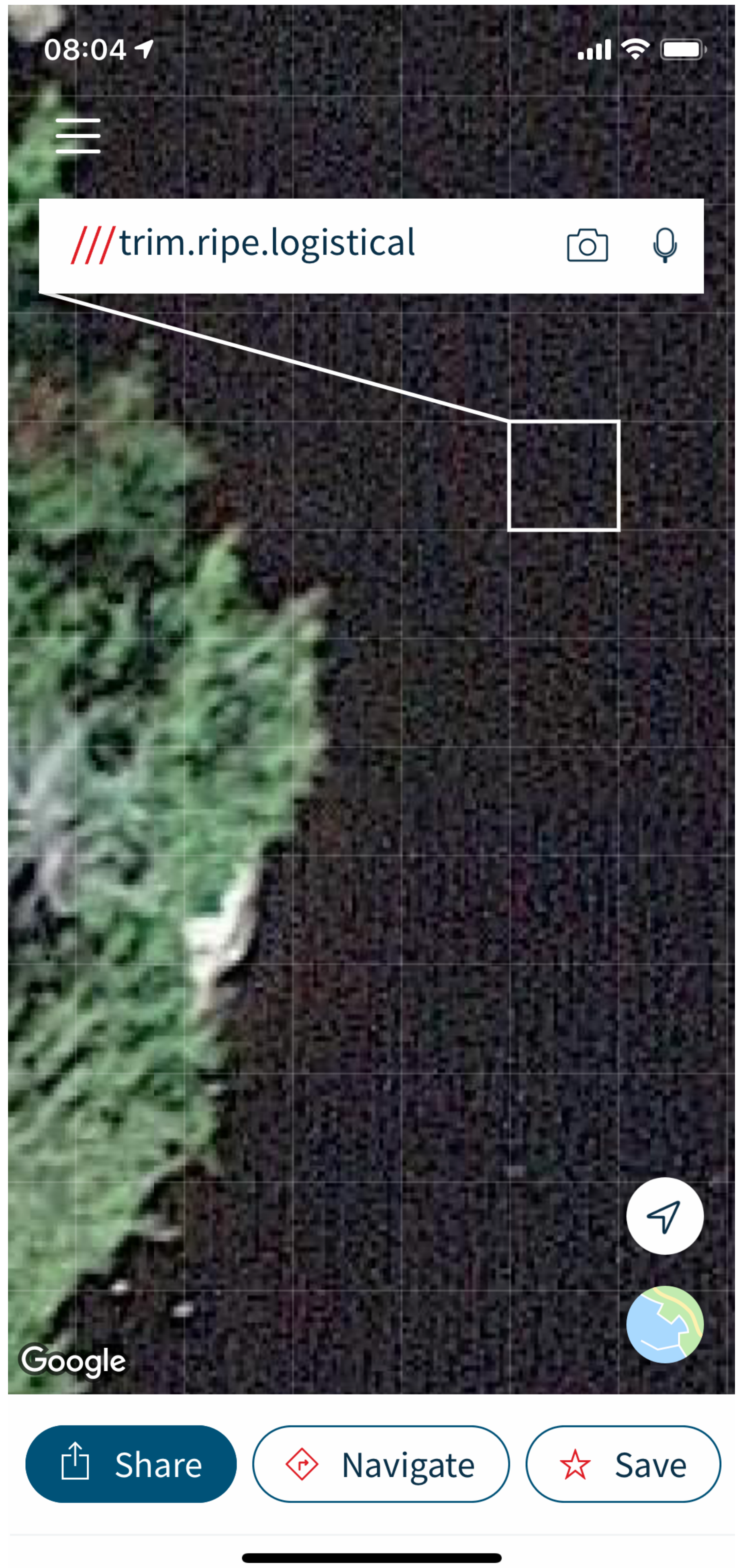
///retailing.practical.improper

The “frog pond” From my youth



///hung.intro.dime

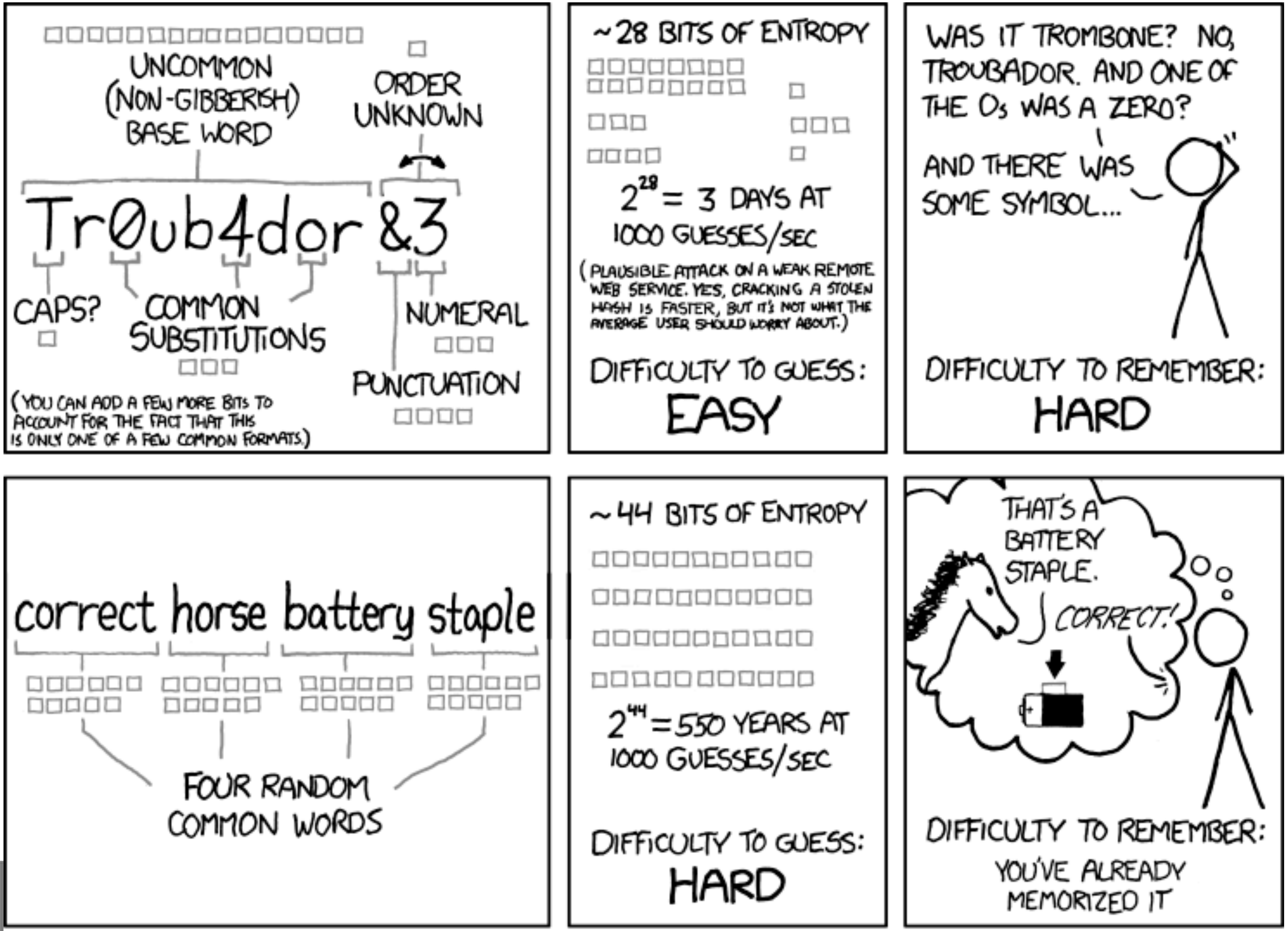
A spot in The Adirondacks



///trim.ripe.logistical

https

https://xkcd.com/936/ Password Strength


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(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.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.

THE MENTOR PROJECT®

https://mentorproject.org

about 100

If you really need “high entropy” passwords

- Not user-chosen, but user can veto, waiting for a “good one”
  - User-chosen phrases have much lower entropy
- They are going to write it down, for a while
- For daily use: who’s going to remember this over a year?

Updated Advice

For Users

Recommendations for users

- **Use three levels of passwords based on importance:**
  - **No importance: NY Times, etc.**
    - But the importance can change when you are not looking!
  - **Inconvenient if stolen: Amazon**
  - **Major problem if abused: bank access, medical records(?)**

For users (cont.)

- Write down the rare ones if you must
  - Don’t write down the password, write a reminder of the password
- Use variations to meet “strong” password requirements.
- Do note required variations (i.e. lower case, no spaces)

Save your passwords in your browser?

- Little difference against keystroke logging
- Key-ring protection mechanisms subject to dictionary attacks
- If stolen, you have given away an authentication factor

Use password vaults, 1password, lastpass, etc.

- They are not perfect, but MUCH better and easier
- Share your authentication with your partner

Engineering goal: The non-moronic password rule!

- Pick something a friend, colleague, or ace hacker won’t guess in a few tries, and they can’t figure out while watching you type it
- This is an easy, obvious security rule we can all agree on

What are the most common current threats

- Keystroke loggers
- Phishing attacks
- Password database compromise

Rethinking Passwords

Bill Cheswick

ches@cheswick.com

https://cheswick.com/ches/talks

THE MENTOR PROJECT®

https://mentorproject.org