Rethinking Passwords

Bill Cheswick

ches@cheswick.com

Visiting scholar, U. Penn.

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.

Golden Rule Health

PASSWORD RULES (Please note the password is case sensitive)

Must contain at least 8 characters.

Must include a number and a letter.
No more than two consecutive characters may be the same.

Passwords must be changed at least every 180 days.

No password may be re-used for a period of 1 year.

3 invalid attempts to login will result in a 30 minute lockout.

Wachovia (now Wells Fargo)

Passwords must be 7-20 characters
Must include at least one letter and one number, with no spaces
Semi-colons cannot be part of a Password
Passwords are case sensitive
Do not use your User ID as your Password

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**).

	length	case sens.	A-Z	a-z	0-9	sym	OK	not OK
Intel	>=8	Yes	R	R	R	ok		␣
Golden Rule	>=8							
Wachovia	7-20	Yes	ok	R		no		
Dart-mouth	8		ok	ok	ok	no		
AT&T Uvers	6-24	Yes	R		R	no	- _	
AT&T GNO	5-8	No						
OAG	7-50	Yes	R		R			␣ ‘ “
War-craft	8-16		R		R			-!”#$
DHS	8-15		R		R			␣
Calnet	9-255		3	3	3	3	␣	
UAL	6-24	No						
Lehigh	>=7		2	2	2	2		

These “eye-of-newt” rules are not user-friendly

- **hard to remember**
- **hard to type**
- **doesn’t increase the search space (password strength) that much**
- **Enforcing these rules excludes genuinely strong and easier pass phrases**

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.**

mail.coastal.cheswick.com login failures:

```
Sep 21 03:11:03 mail sshd[90325]: Invalid user cgi from 219.139.108.134
Sep 21 03:11:15 mail sshd[90335]: Invalid user oracle from 219.139.108.134
Sep 21 03:11:18 mail sshd[90337]: Invalid user tomcat from 219.139.108.134
Sep 21 03:11:47 mail sshd[90361]: Invalid user nagios from 219.139.108.134
Sep 21 04:50:29 mail sshd[54849]: Invalid user devtest from 58.213.48.82
Sep 21 04:50:33 mail sshd[54851]: Invalid user dede from 58.213.48.82
Sep 21 04:51:49 mail sshd[54895]: Invalid user anja from 58.213.48.82
Sep 21 04:51:55 mail sshd[54897]: Invalid user anja from 58.213.48.82
Sep 21 04:51:59 mail sshd[54899]: Invalid user platinum from 58.213.48.82
Sep 21 04:52:03 mail sshd[54901]: Invalid user plcmspip from 58.213.48.82
Sep 21 04:52:06 mail sshd[54903]: Invalid user teamcity from 58.213.48.82
Sep 21 04:52:13 mail sshd[54905]: Invalid user teamspeak from 58.213.48.82
Sep 21 04:59:33 mail sshd[55143]: Invalid user addr from 58.213.48.82
Sep 21 04:59:37 mail sshd[55145]: Invalid user adempiere from 58.213.48.82
Sep 21 04:59:40 mail sshd[55147]: Invalid user admin2 from 58.213.48.82
Sep 21 04:59:43 mail sshd[55149]: Invalid user admin from 58.213.48.82
Sep 21 04:59:57 mail sshd[55157]: Invalid user admin from 58.213.48.82
Sep 21 05:00:02 mail sshd[55159]: Invalid user admin from 58.213.48.82
Sep 21 05:00:05 mail sshd[55177]: Invalid user adminftp from 58.213.48.82
Sep 21 05:00:08 mail sshd[55179]: Invalid user adminhelp from 58.213.48.82
Sep 21 05:00:12 mail sshd[55181]: Invalid user admin from 58.213.48.82
Sep 21 05:00:15 mail sshd[55183]: Invalid user admin from 58.213.48.82
```

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 on each System

Change Your Password Frequently

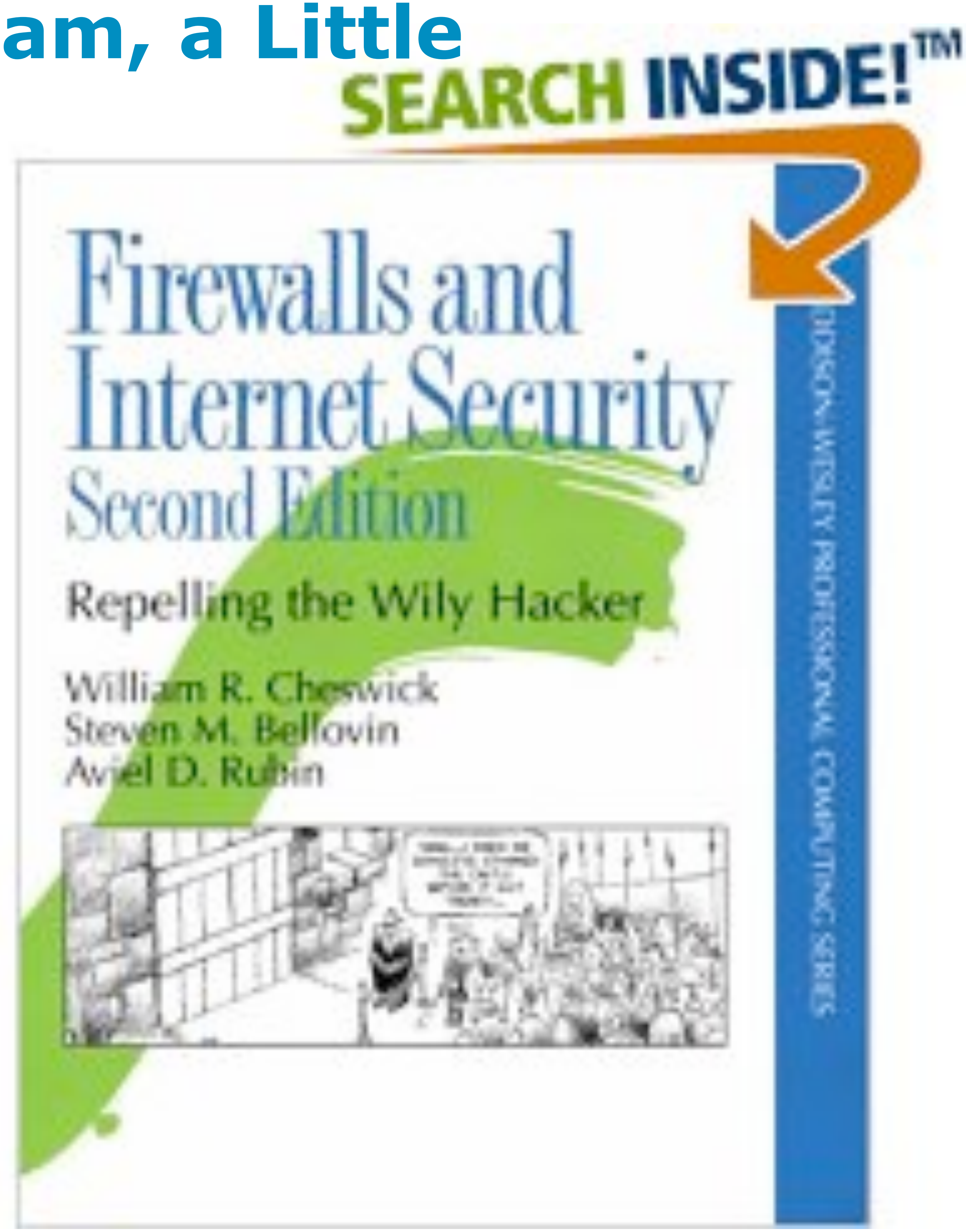
Don’t Reuse Passwords

Don’t Write Your Password Down

This is a usability nightmare!

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

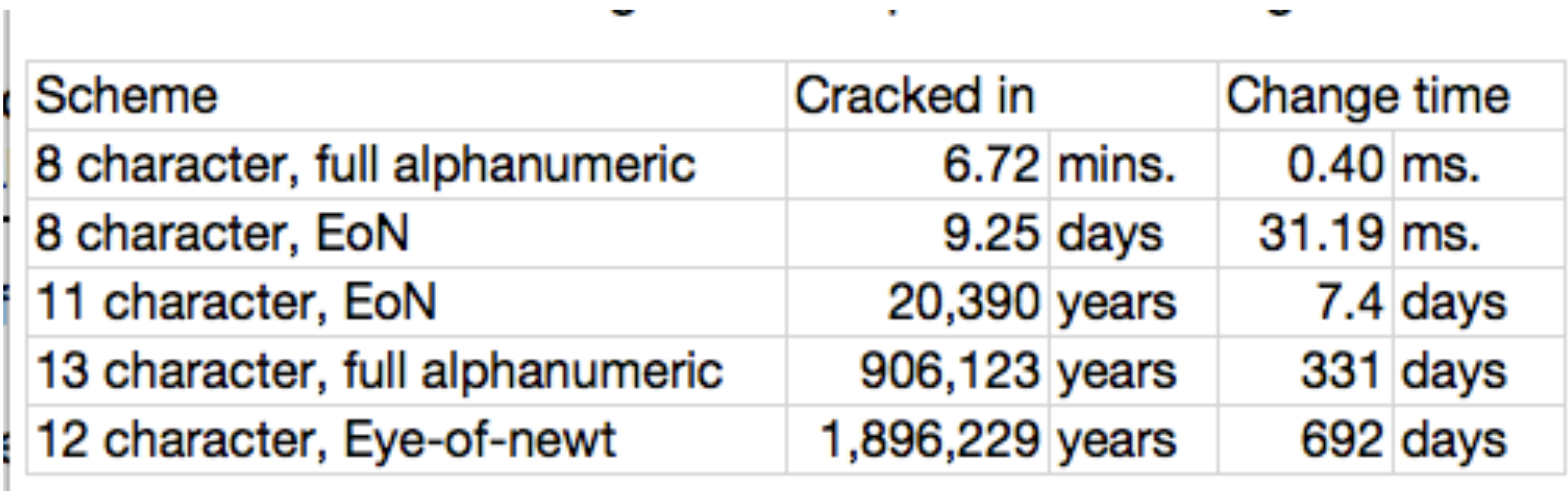
ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

What are these rules for?

Dictionary Attacks

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

- **The “green book”.**
- **A variety of mostly-excellent security suggestions**



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

Where Do Security Policies Come From?

Dini Florêncio and Cormac Herley

SOUPS 2010

Those that accept advertising, purchase sponsored links, or user has a choice have weakest password requirements

Strongest passwords: .gov, then .edu

These rules come from the Deep Past in computing and security

- Time sharing terminals in public places
- Attacks on the login interfaces on network services
- Network eavesdropping was often trivial
- The stakes were usually much lower
- Institutionalized passwords on, say, telephone switches
- Changing passwords: lost military crypto gear

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!

Security people are paid to think bad thoughts - Bob Morris

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.

What are the most common current threats

- **Keystroke loggers**
- **Phishing attacks**
- **Password database compromise**
- ***NOT DICTIONARY ATTACKS!***

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

Results

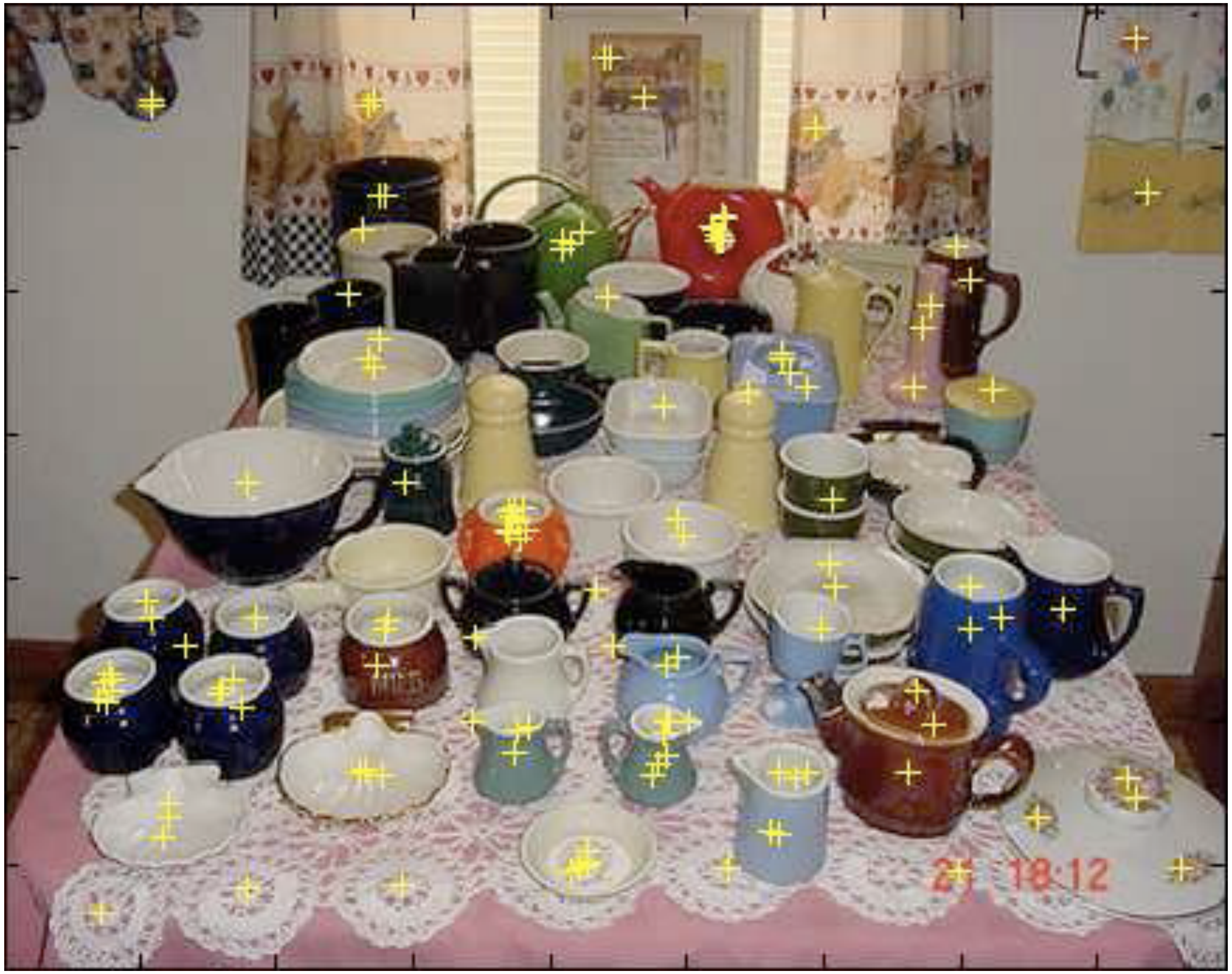
- People violate many of these rules routinely, for usability reasons
- Stringent rules increase use of fall-back systems, which are usually less secure, or more expensive
- The rules don’t make most things more secure in the face of most current threats

Some Password Ideas

From academia, and me

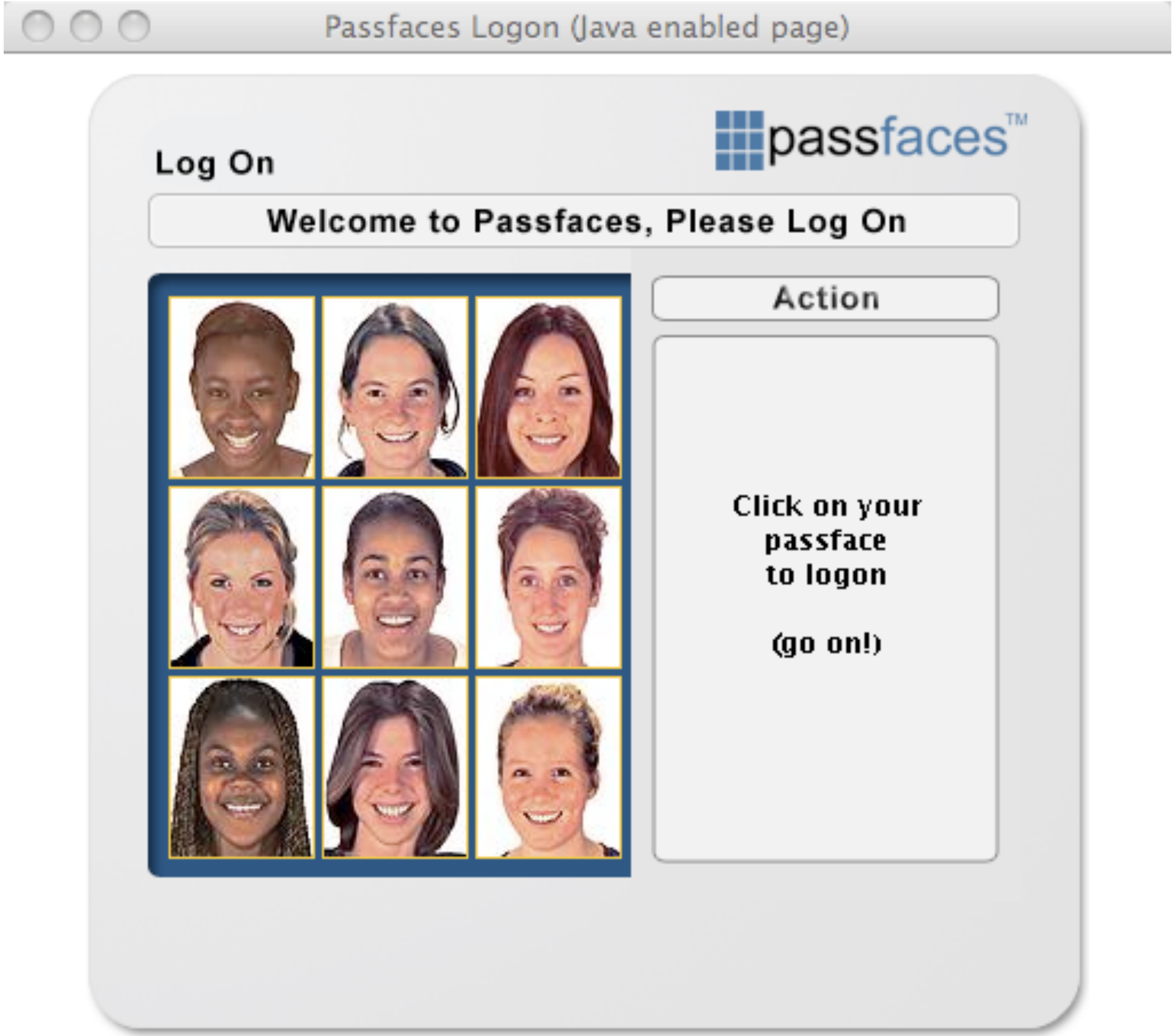
For a complete survey, see

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



from Dirik, Memon, Birget; SOUPS 2007

Passfaces

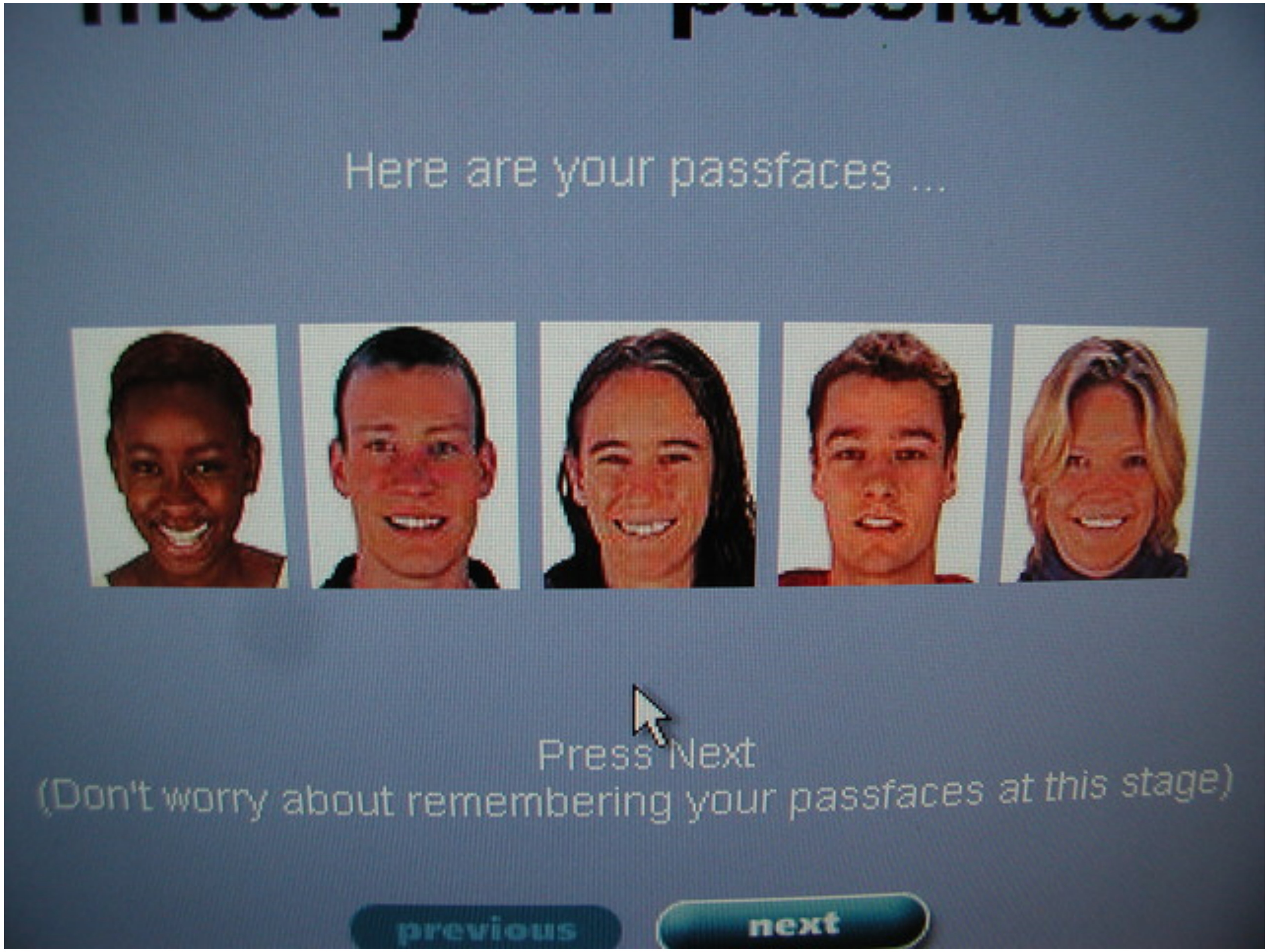


Welcome to Passfaces, Please Log On

Click on your
passface
to logon

(go on!)

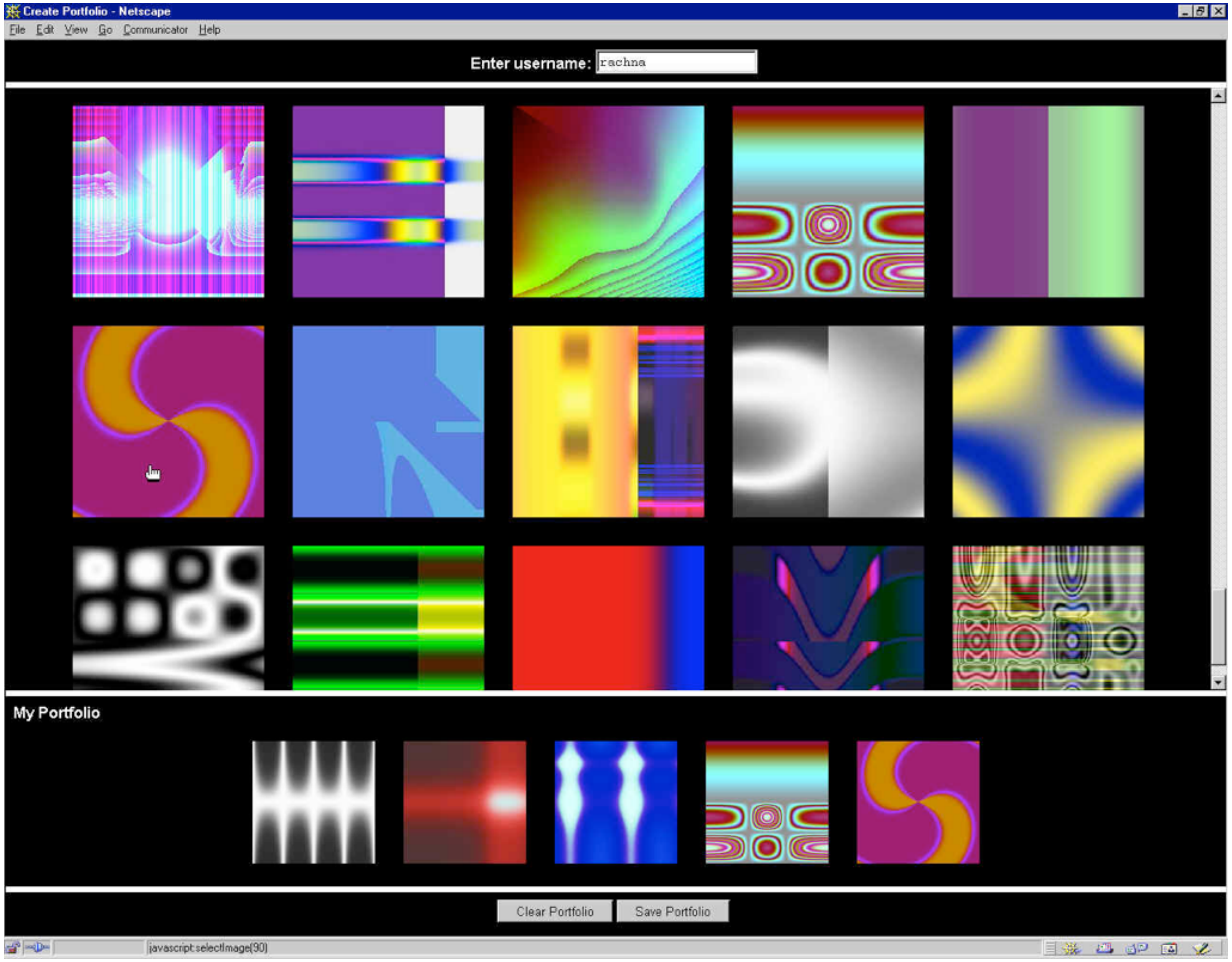
My passfaces



Here are your passfaces ...

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

Deja Vu (Recognition-based)



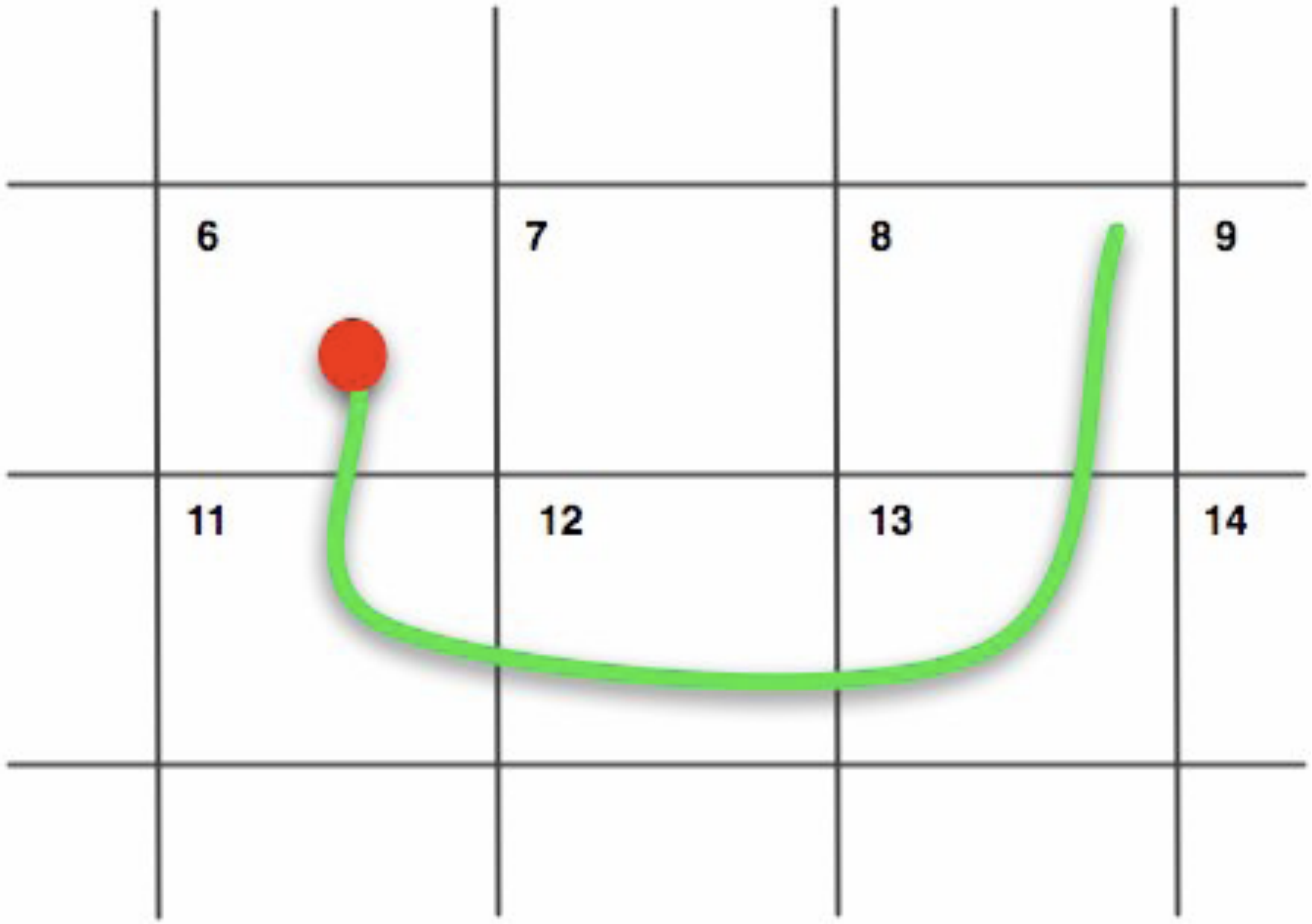
Create Portfolio - Netscape
File Edit View Go Communicator Help
Clear Portfolio
Save Portfolio

Enter username: rachna

My Portfolio

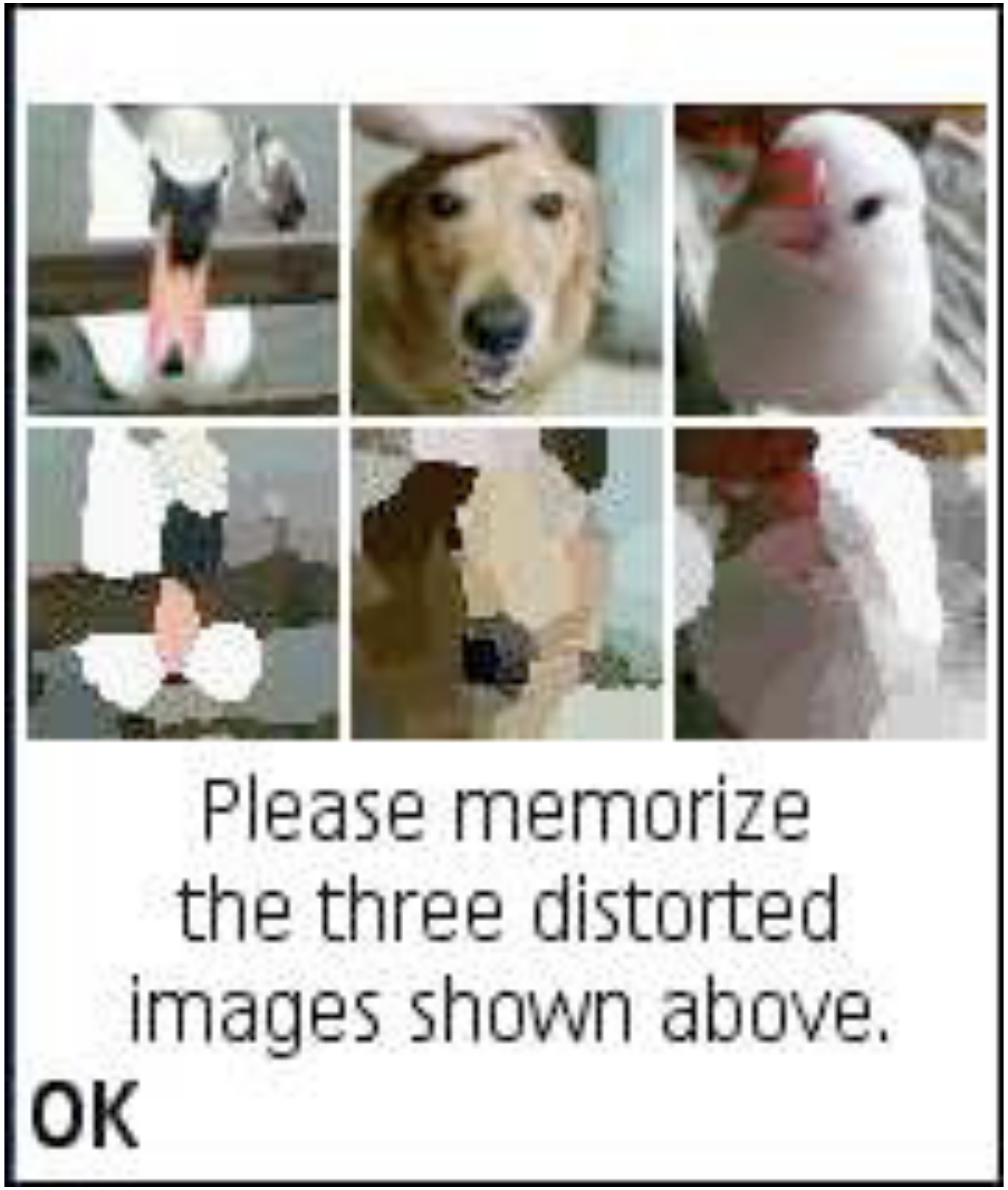
javascript:selectImage(90)

Draw a Secret



Lin, Dunphy, et al. SOUPS 2007

Use Your Illusion (SOUPS 2008)



Please memorize the three distorted images shown above.

Another Solution: Don’t allow common passwords

Popularity* is *Everything

Stuart Schechter, Cormac Herley, Michael Mitzenmacher;

HOTSEC 2010.

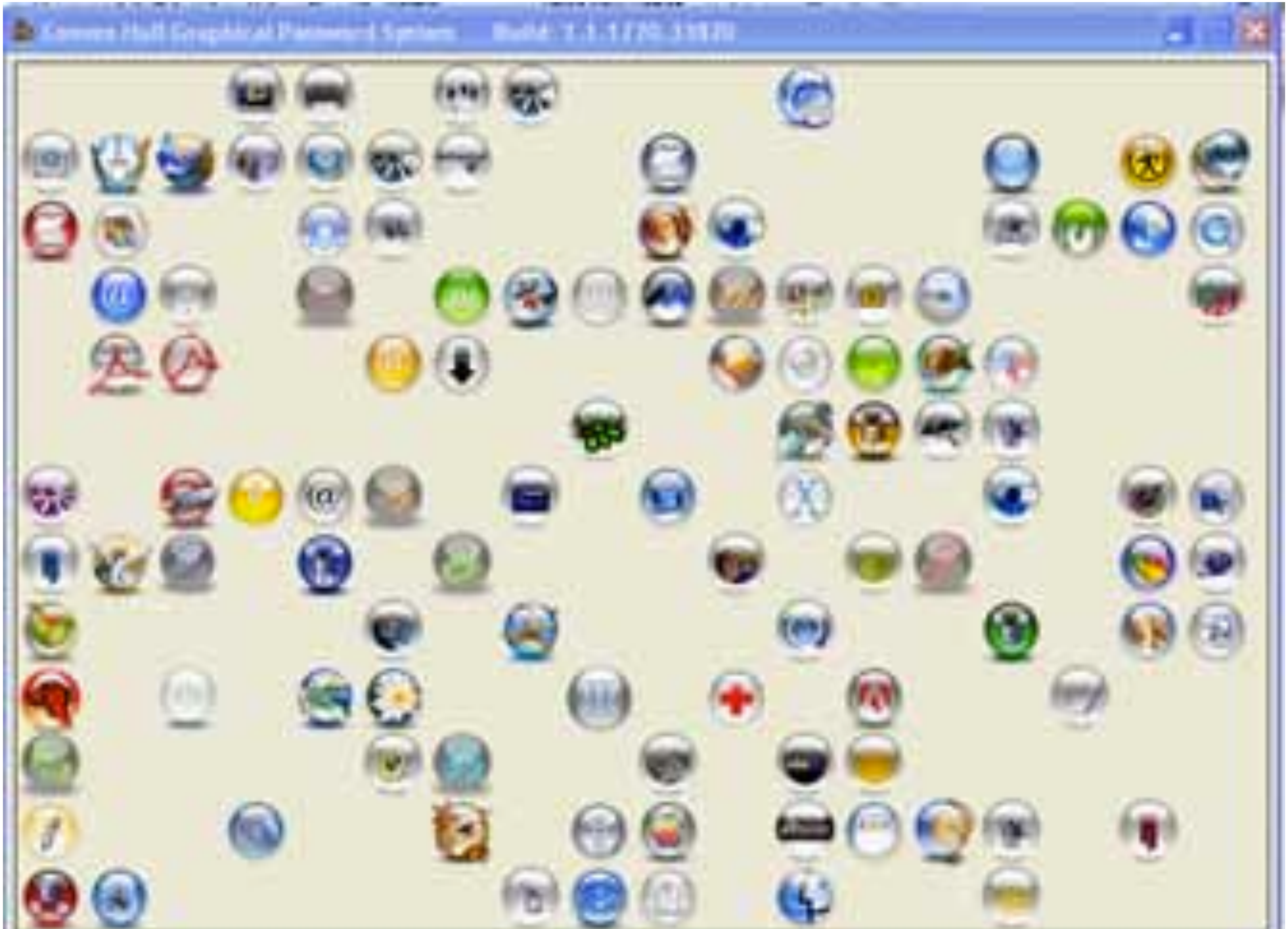
Count and limit password choices

- **I.E. only 100 people (out of a million?) may use *password* as a password**
- **Makes the dictionary attack much harder: common targets vanish**
- **Makes passwords harder to choose, like picking a gmail account name: *dragonslayer6478***

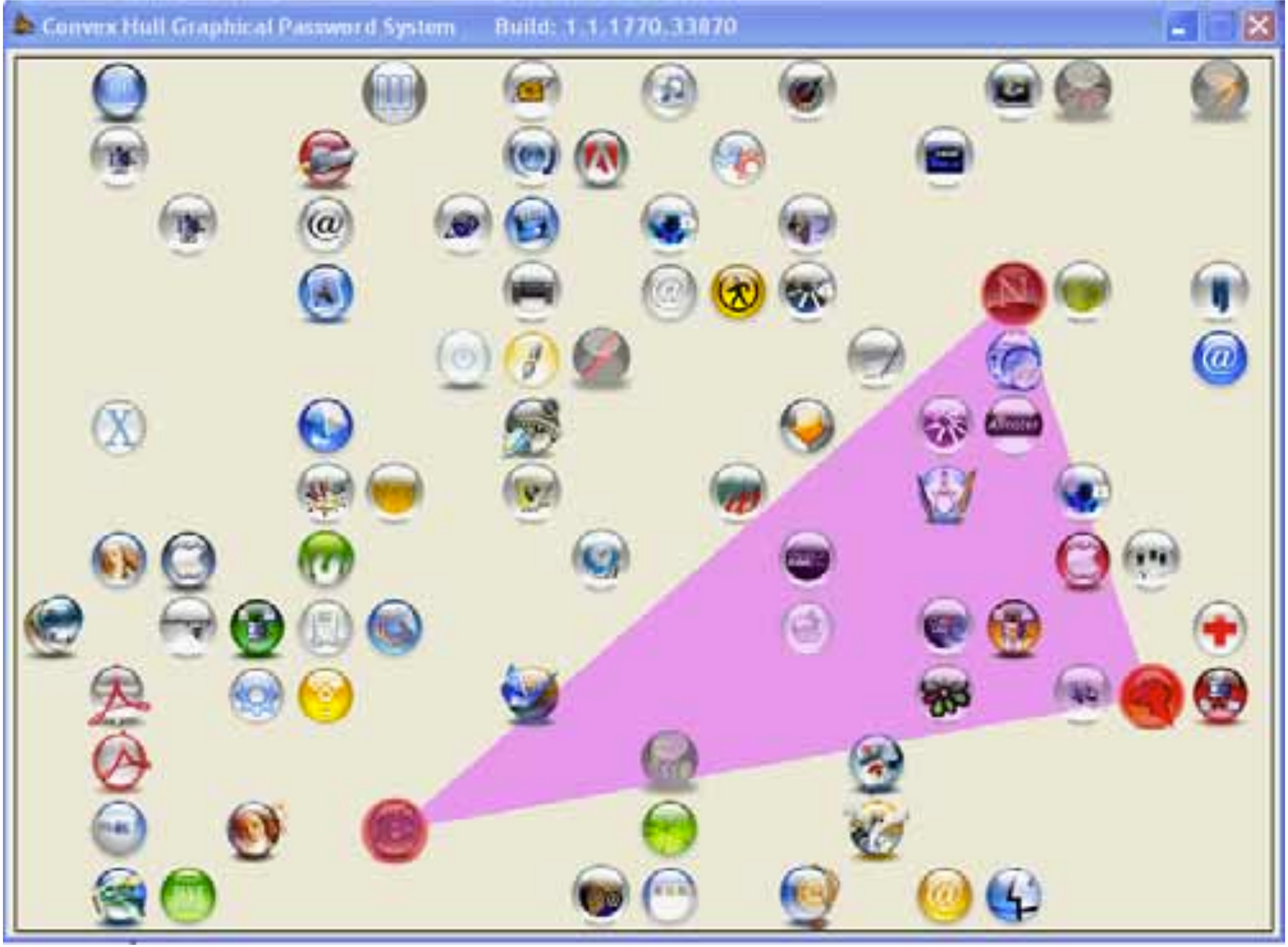
Convex hull formed by known icons

- S. Wiedenbeck, J. Waters, L. Sobrado, J.C. Birget, ``Design and evaluation of a shoulder-surfing resistant graphical password scheme'', in *Proceedings of Advanced Visual Interfaces (AVI2006)*, Venice, Italy, 23-26 May 2006.
- Our icons:

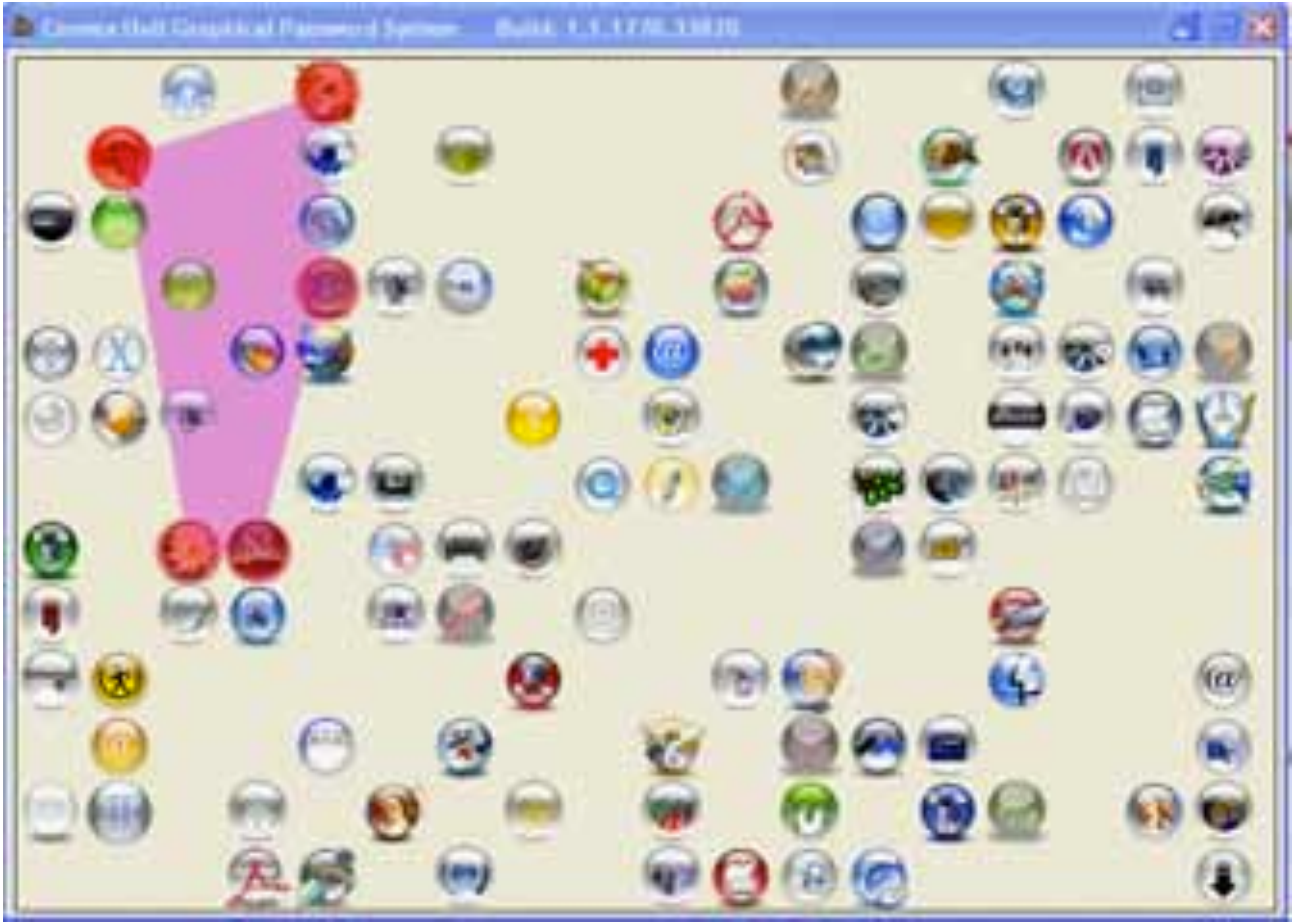
Challenge is a sea of icons


Convex Hull Graphical Password System   Build: 1.1.1720.33920

Find at least three of “your” icons



Do it several times


Convex Hull Graphical Password System   Build: 1.1.1770.13820

Comments

- **What is the entropy, really?**
- **Challenge/response is good**
- **Needs graphics, not text-only**
- **Takes a while to login**

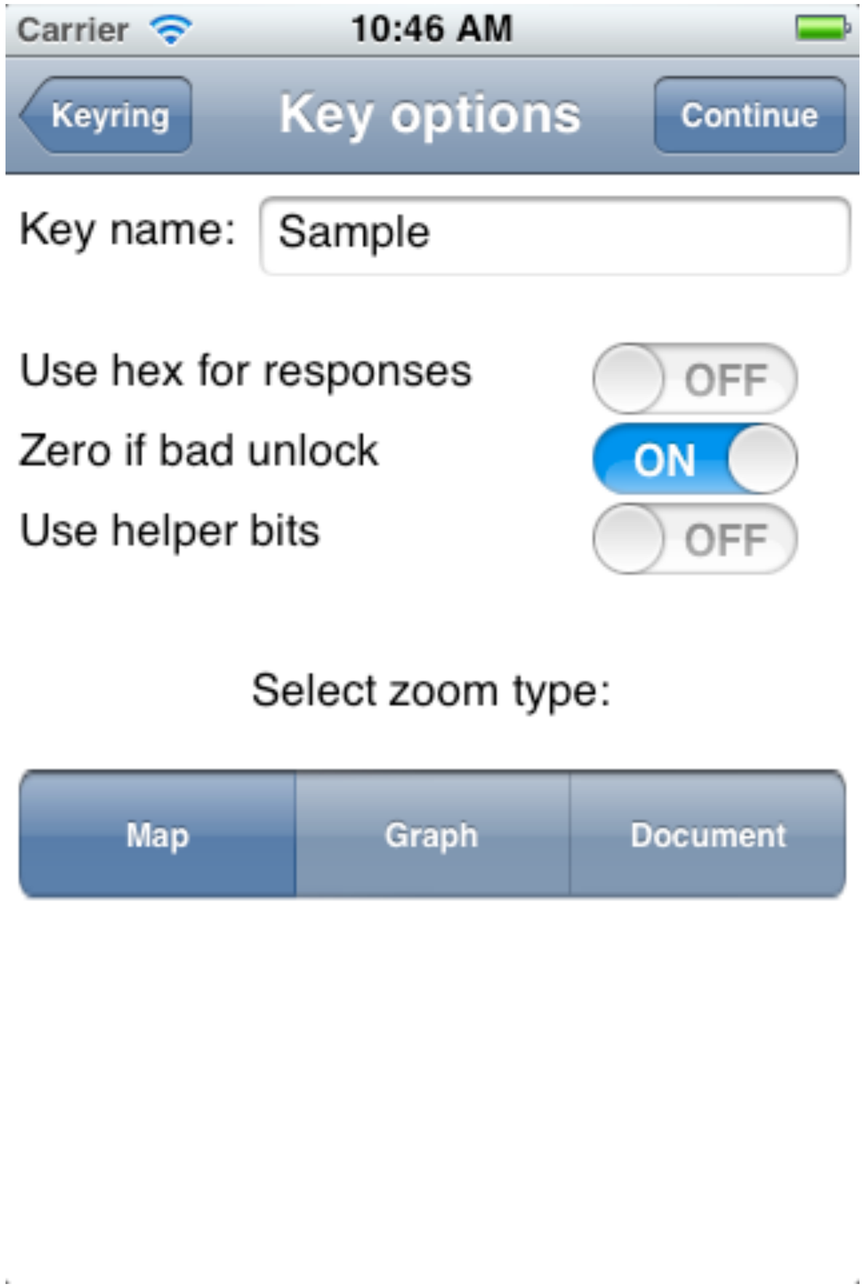
Authentication schemes in general

- **Work factor is hard for usable systems**
- **High work factor systems are usually hard**
- **User studies are required**
  - **uses college kids, two department secretaries, and someone’s grandma**
  - **results seldom surprising (to me, at least)**
- **Mechanical Turk can give much higher N, but tests are hard to create.**

Some Whacko Ideas from ches

Passmaps

(Zoomauth demo)



Key name: Sample

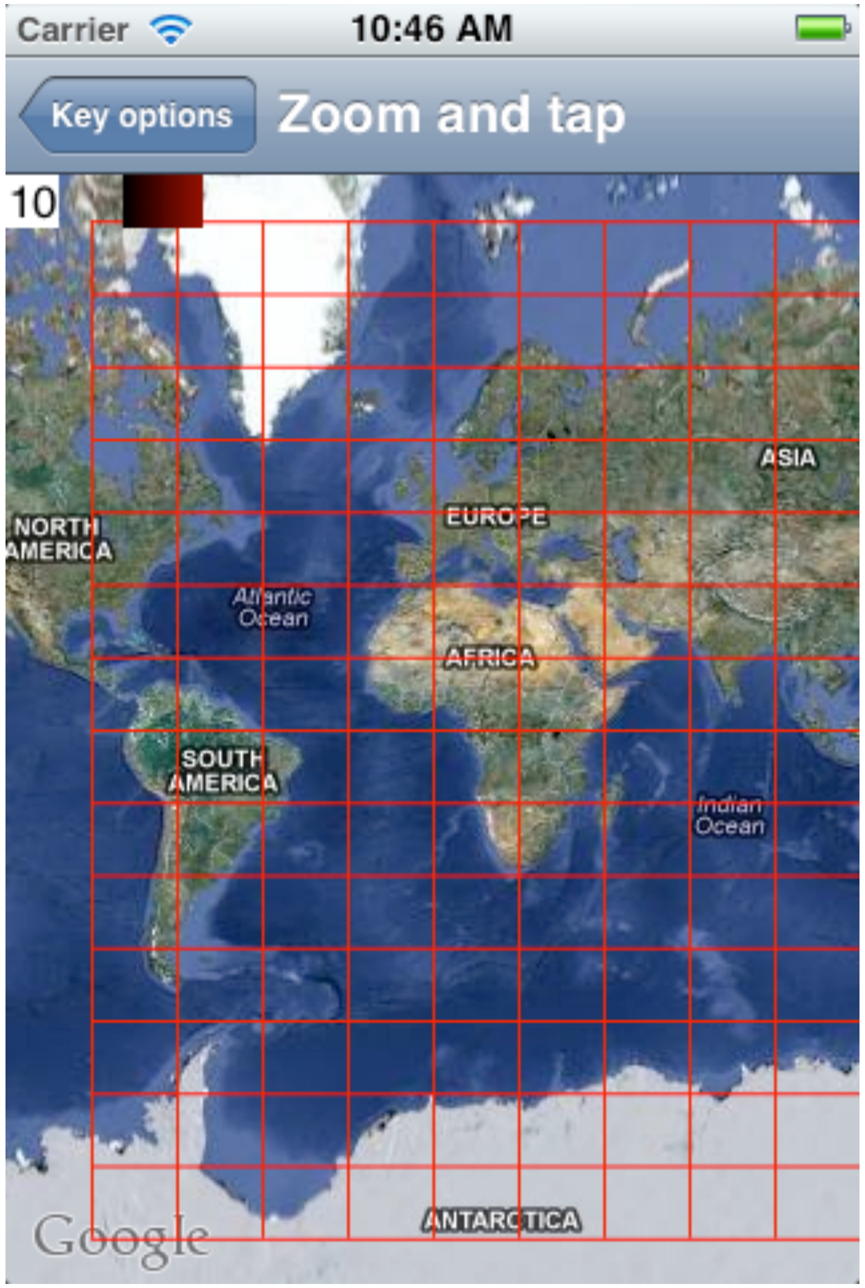
Use hex for responses OFF

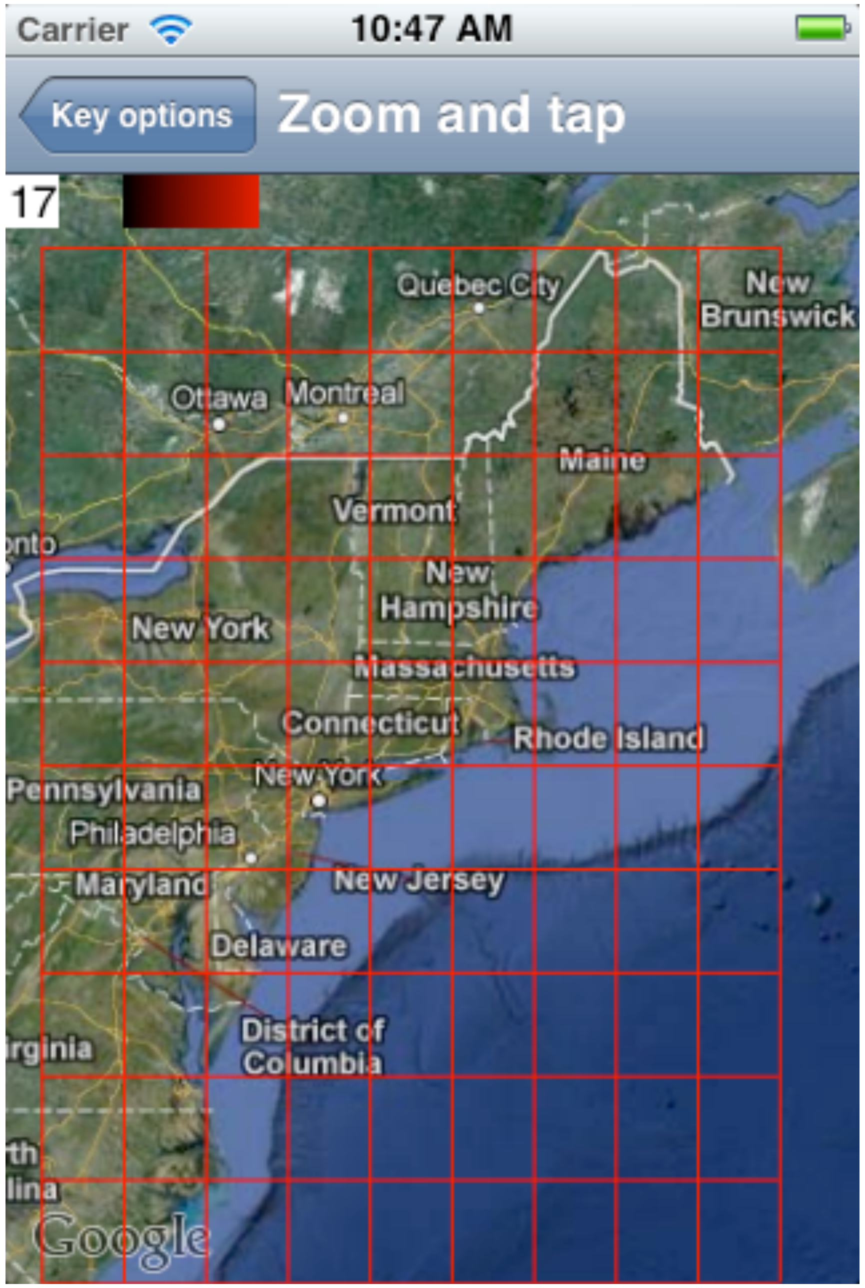
Zero if bad unlock ON

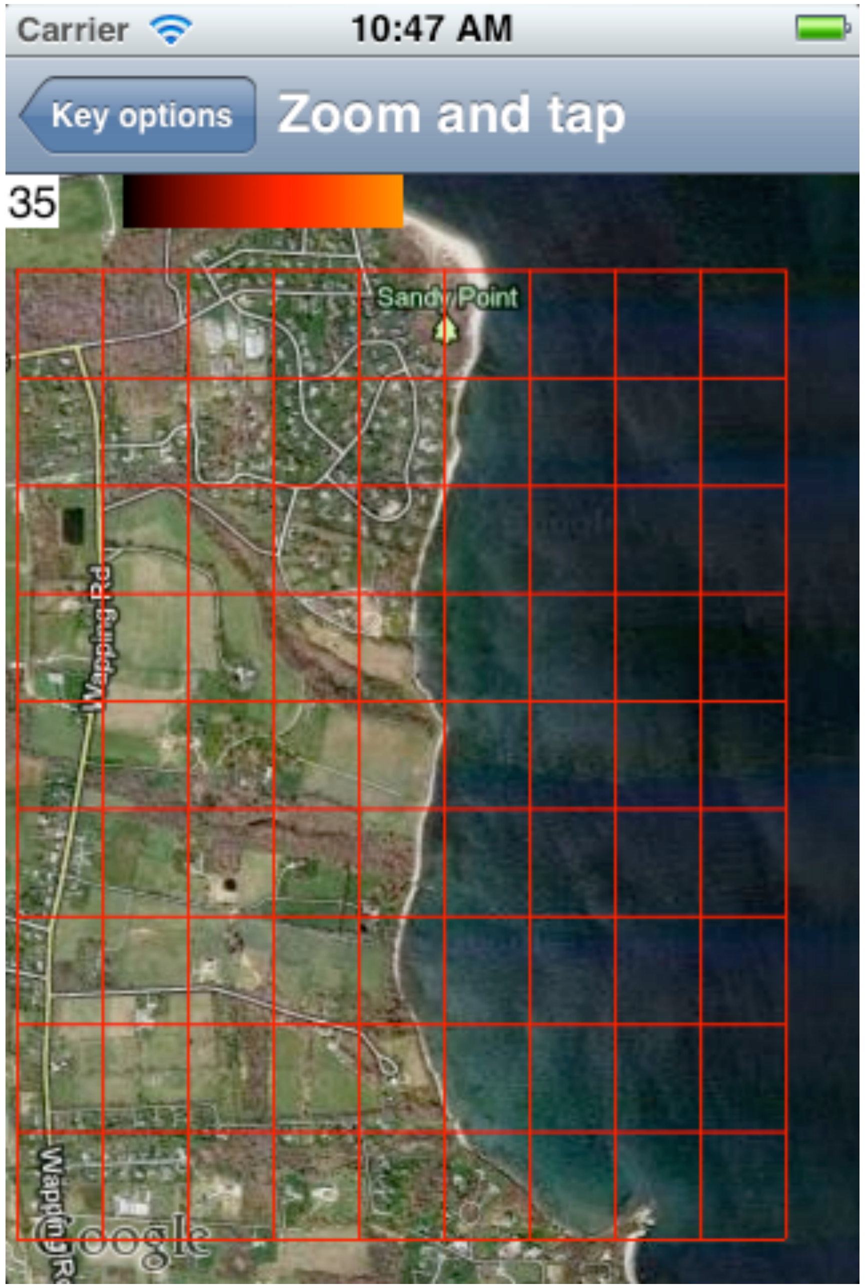
Use helper bits OFF

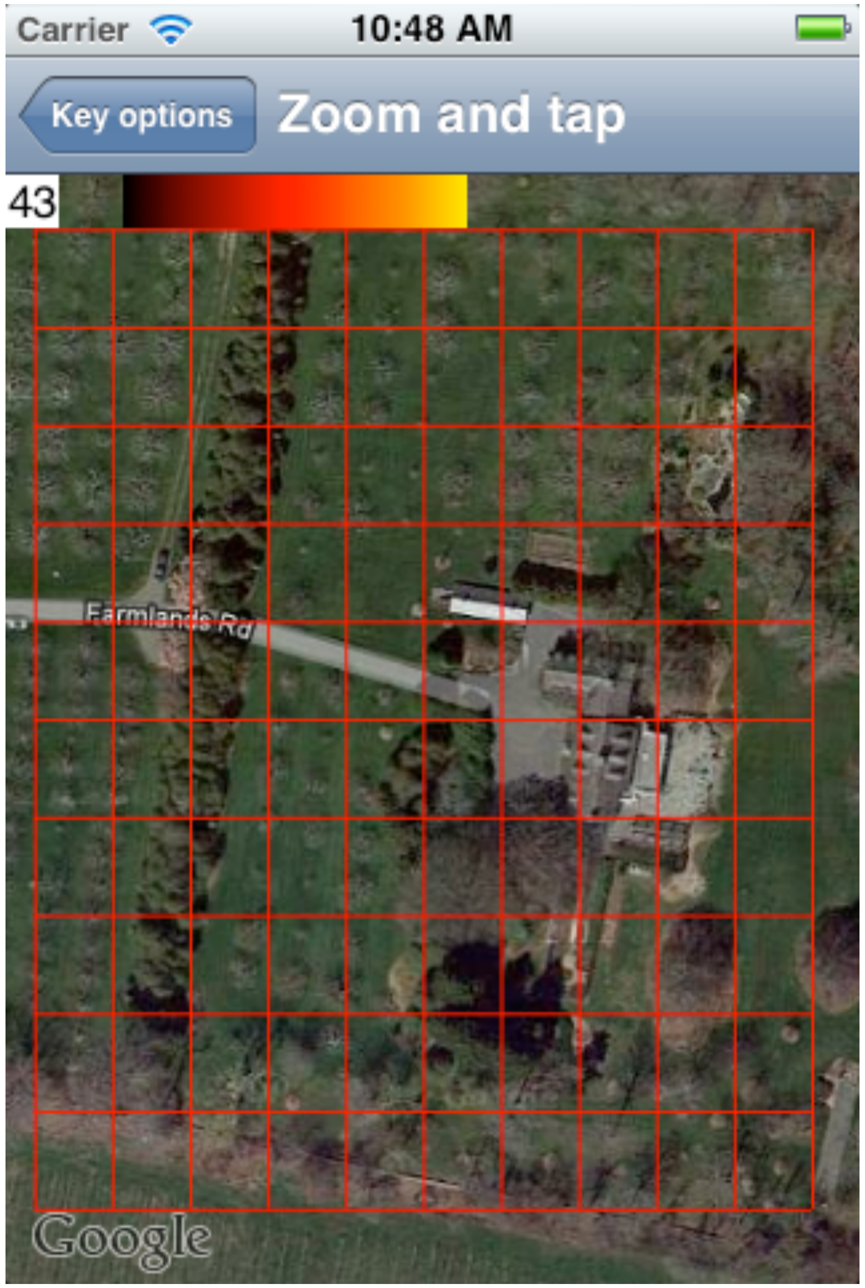
Select zoom type:

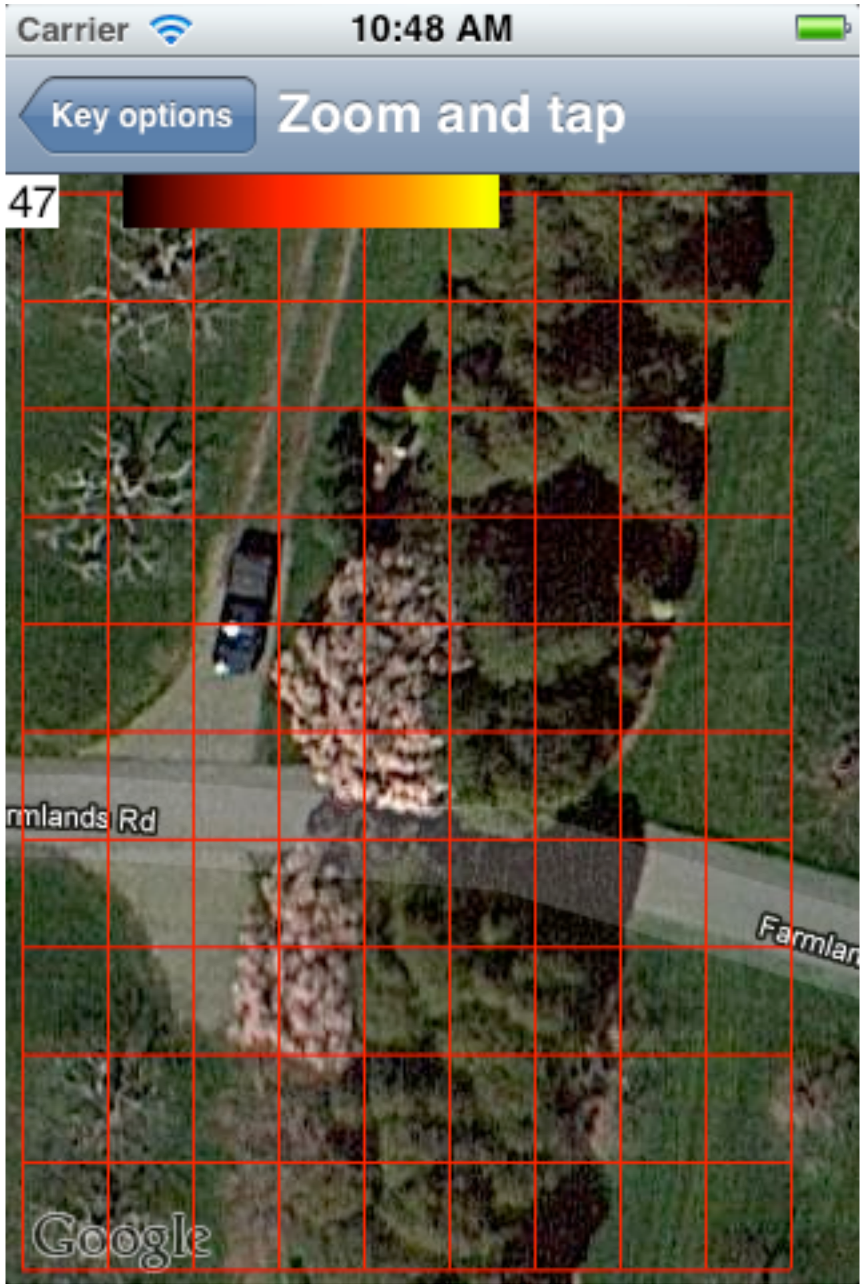
[✓ Map] Graph Document

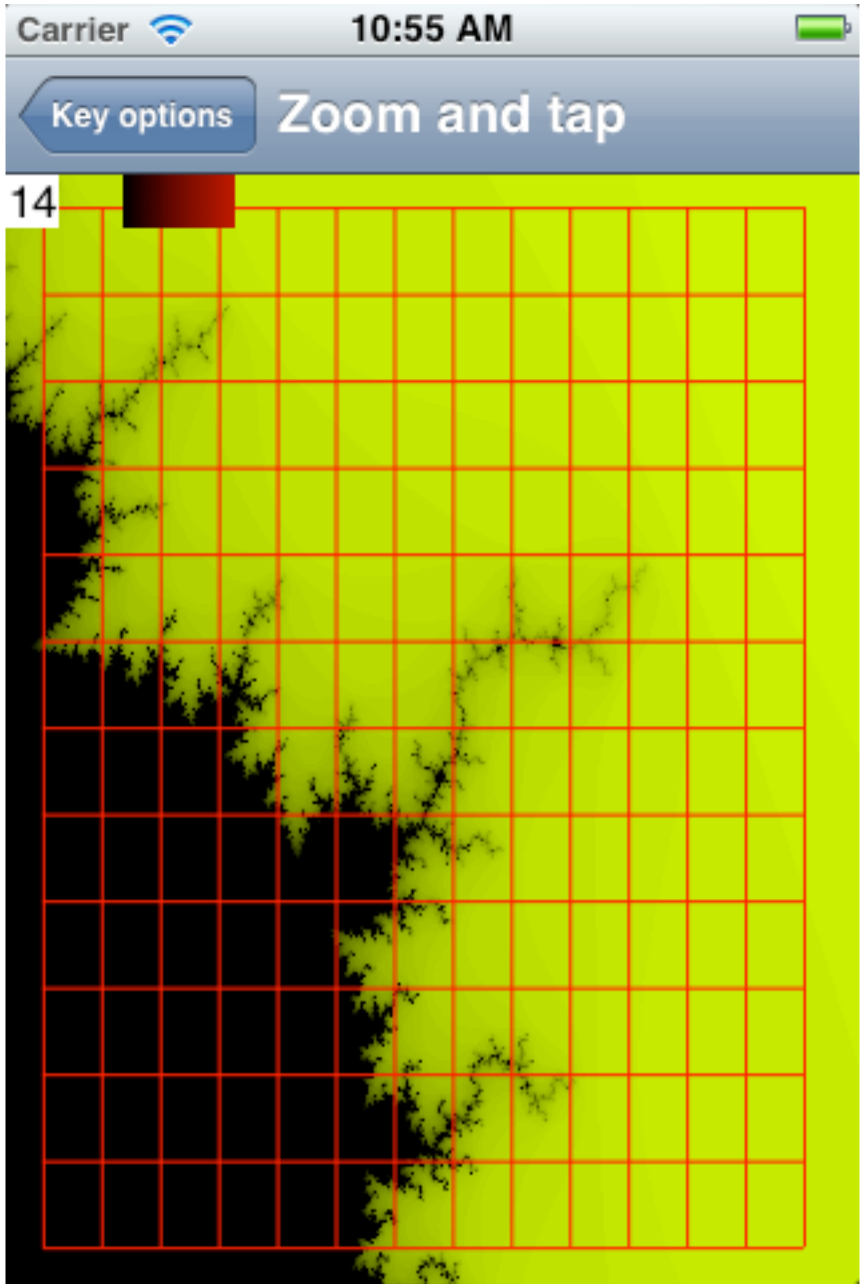


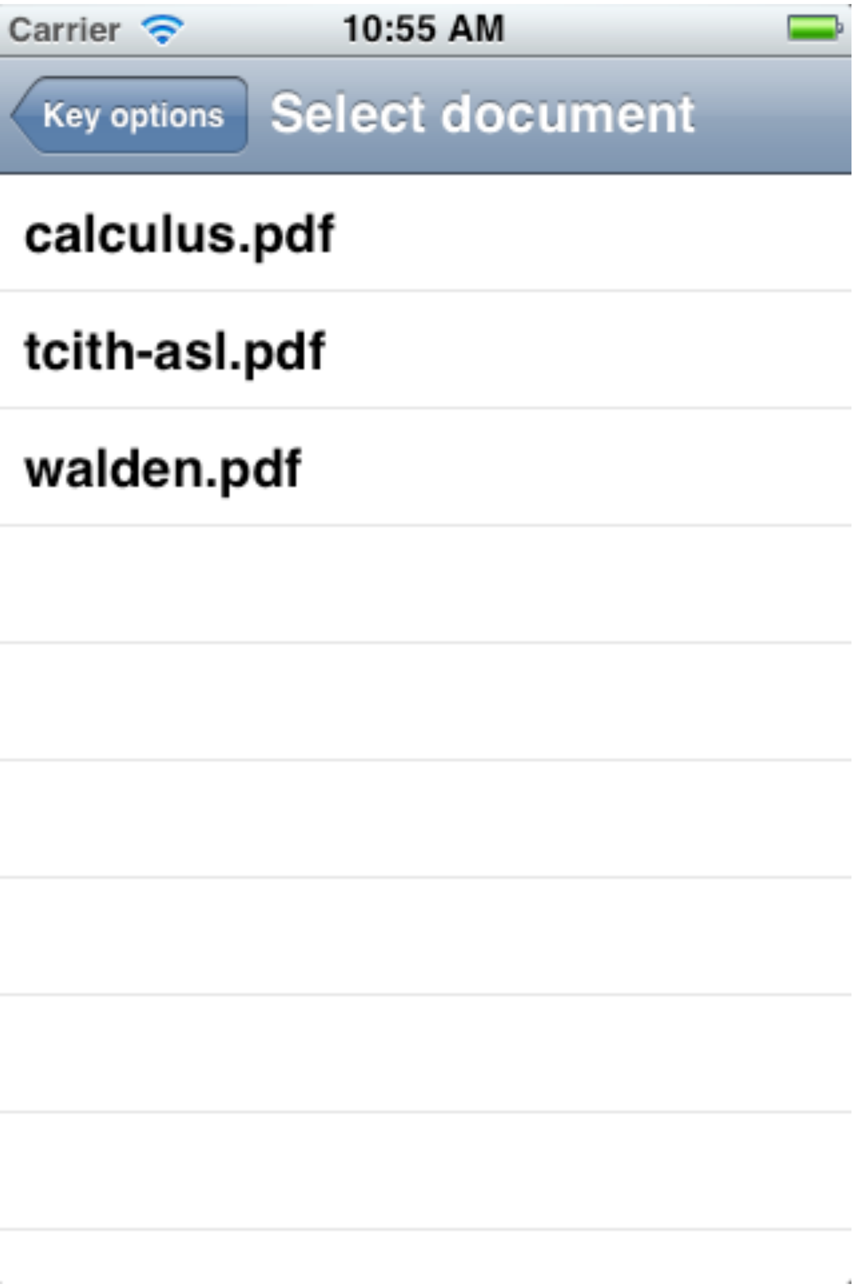


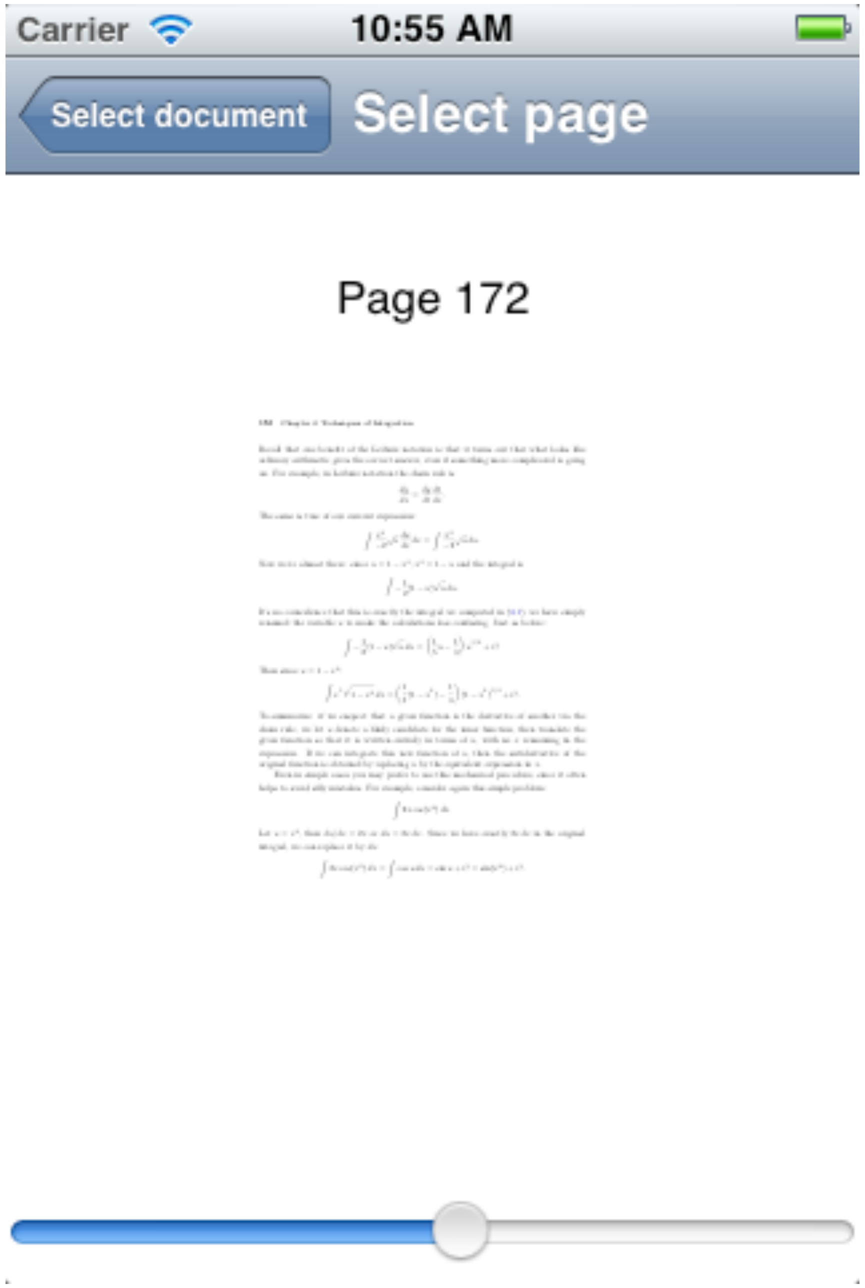

Carrier
10:47 AM
Key options
Zoom and tap
35
Sandy Point
Wapping Rd
Wapping Rd
Google

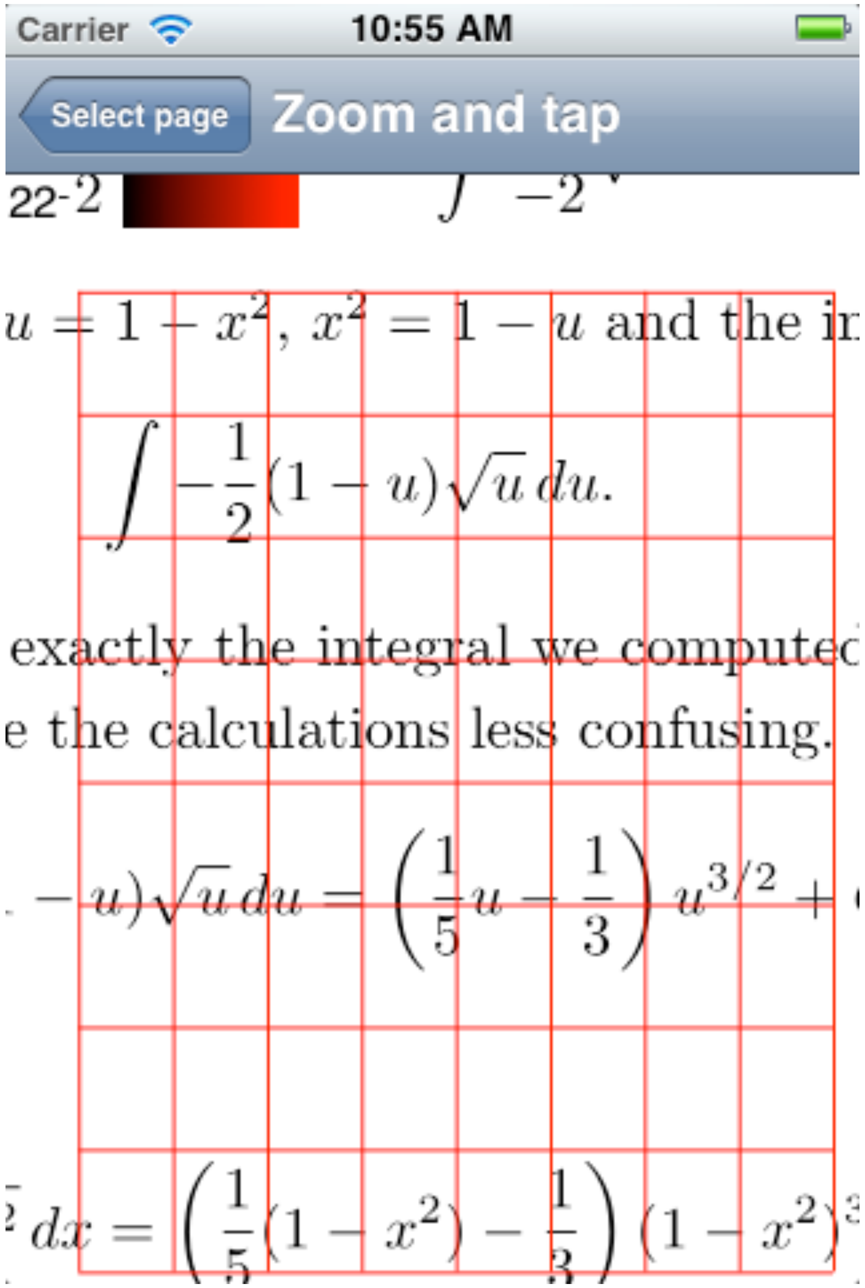

Carrier
10:48 AM
Key options
Zoom and tap
43
Farmlands Rd
Google


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


Carrier
10:55 AM
Key options
Zoom and tap
14







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

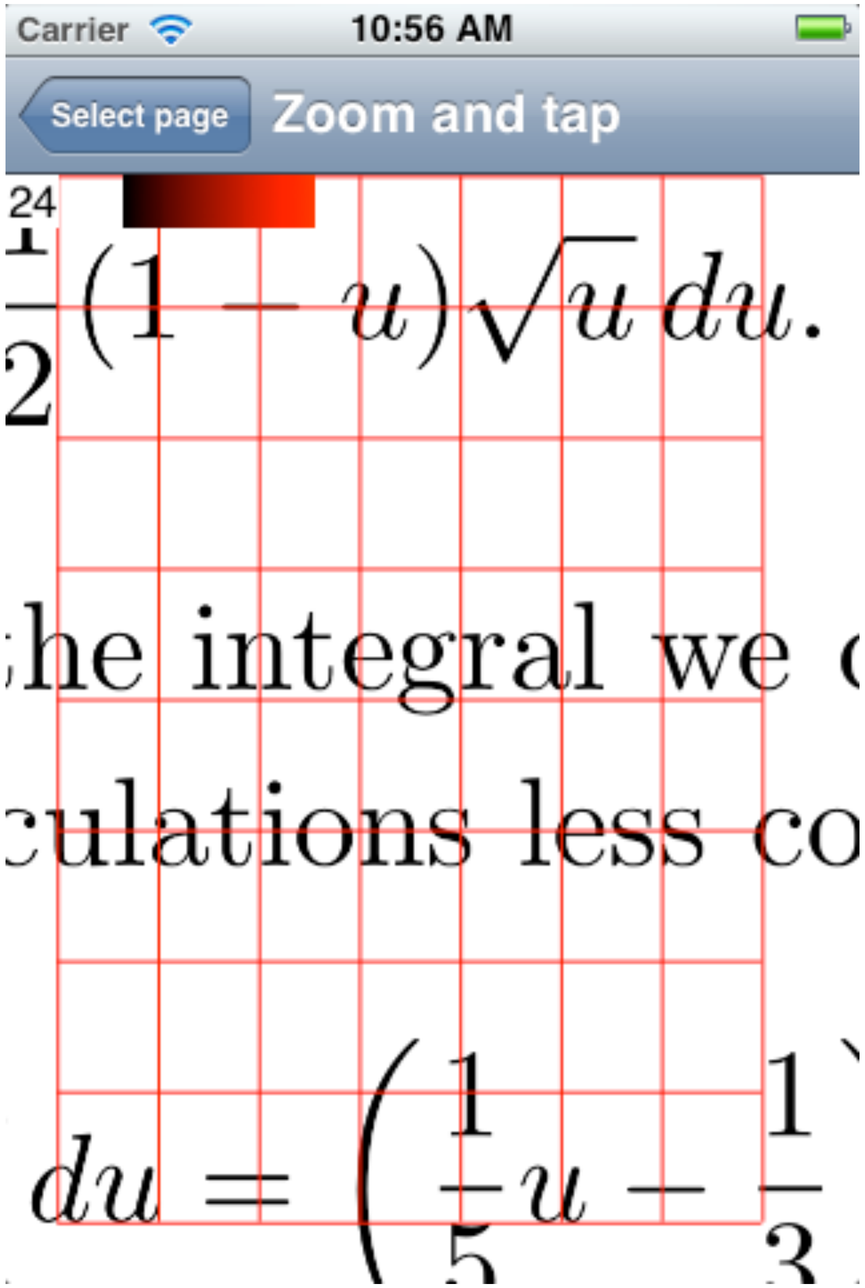
$$\int -\frac{1}{2}(1-u)\sqrt{u}\,du.$$

exactly the integral we computed

e the calculations less confusing.

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

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

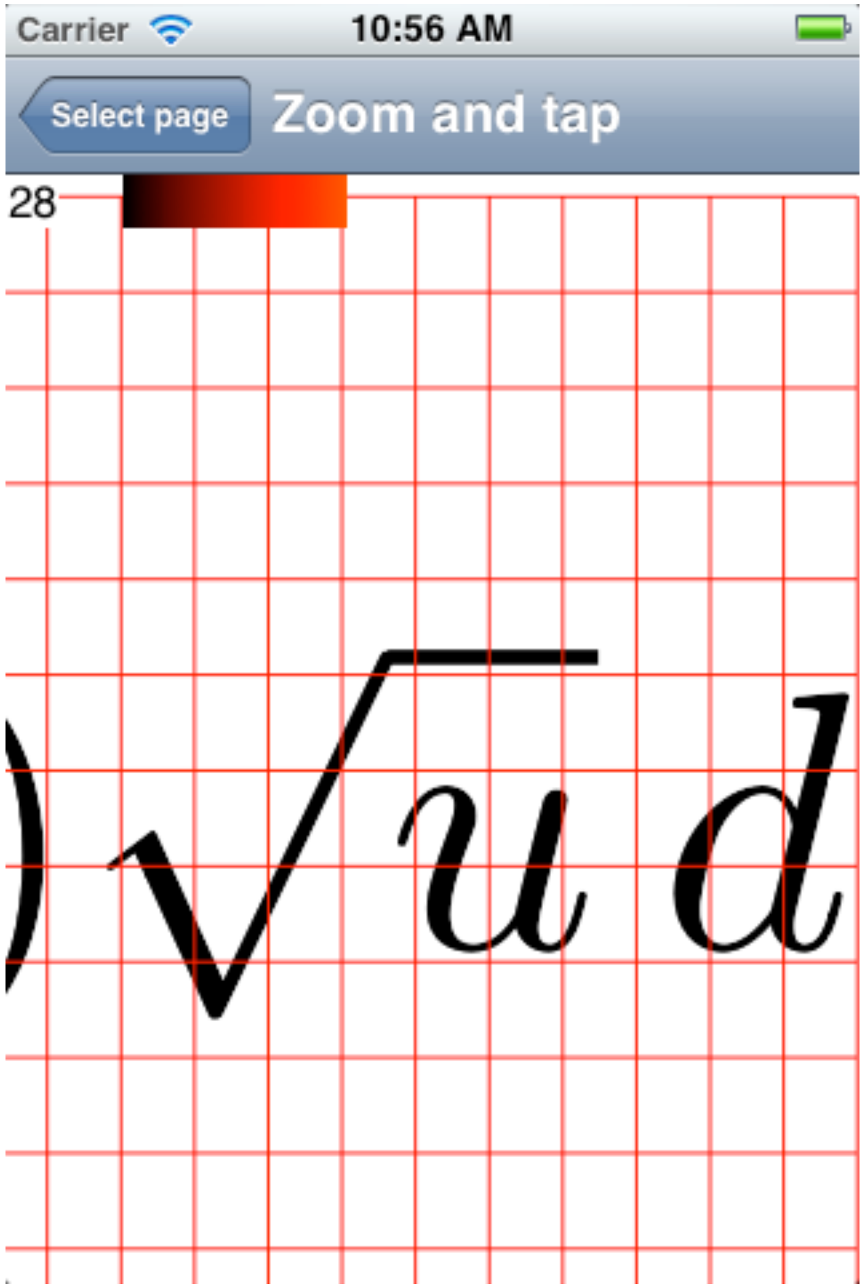


$\frac{1}{2}(1-u)\sqrt{u}\,du.$

he integral we c

culations less co

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



$)\sqrt{u}\,d$

Some Whacko ches Ideas

Obfuscated human-computed challenge response

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
210
4
NIA INSURANC

210
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]

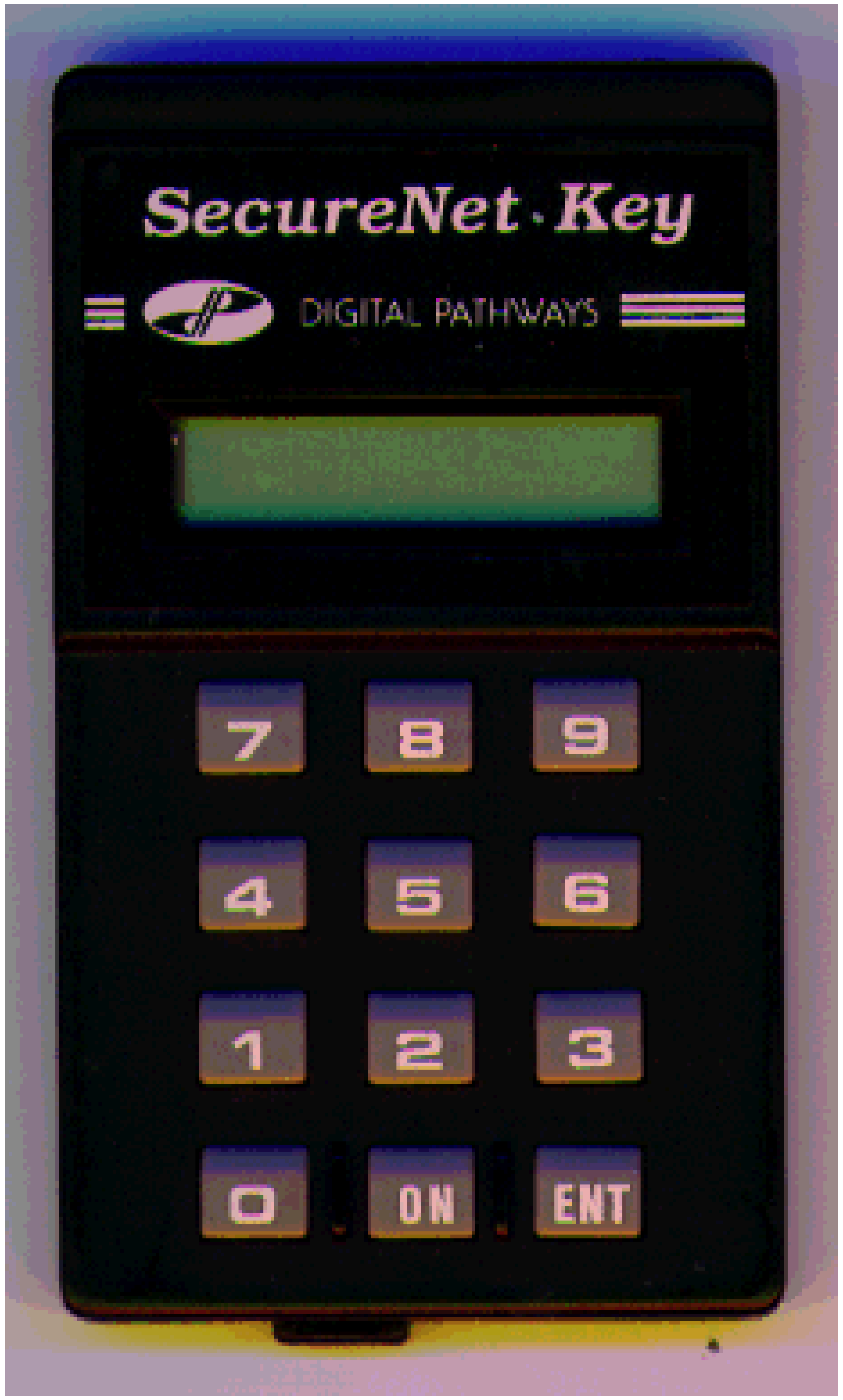
Can “something you know be saved?”

- 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
  - .....

Better Solutions

#1: Getting out of the game

SecureNet Key SNK-004

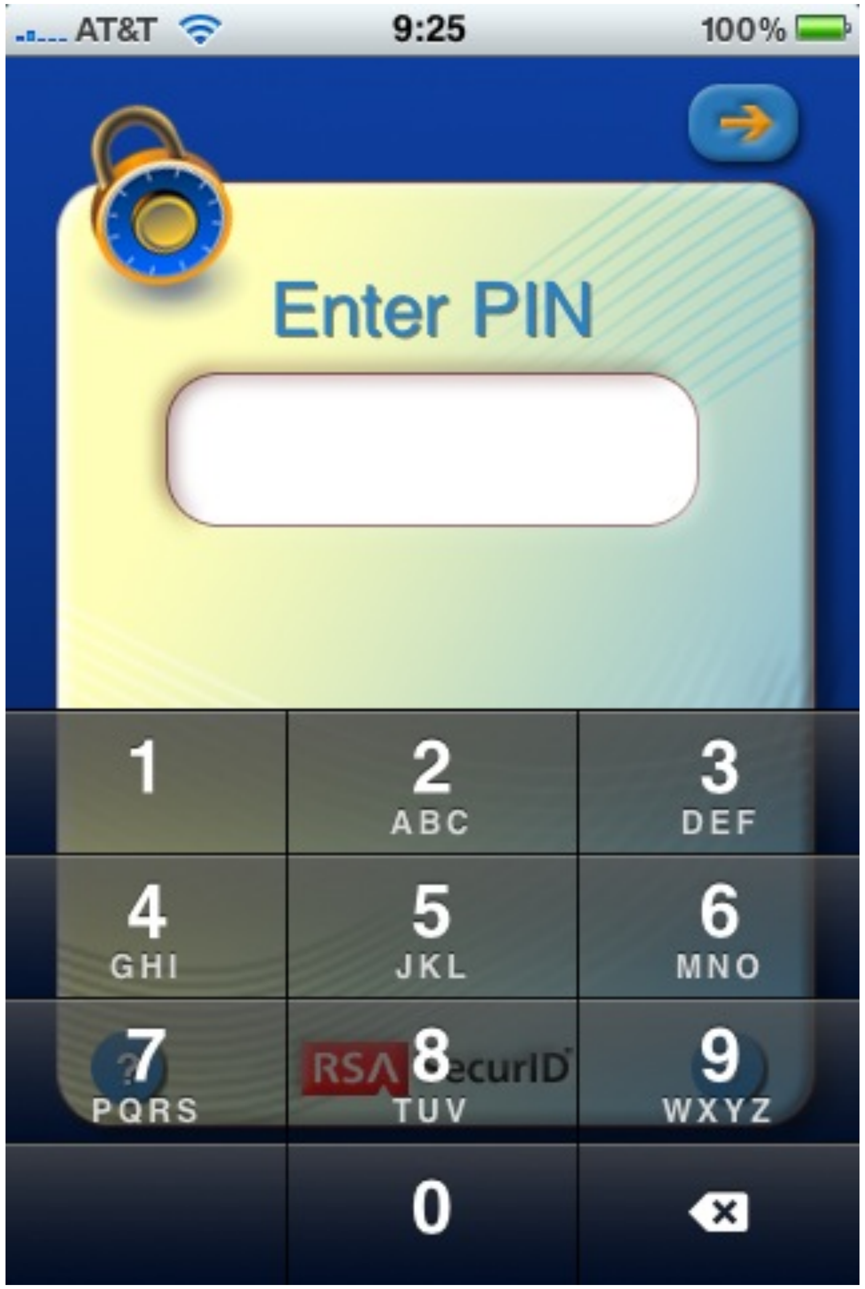


A login from my distant past

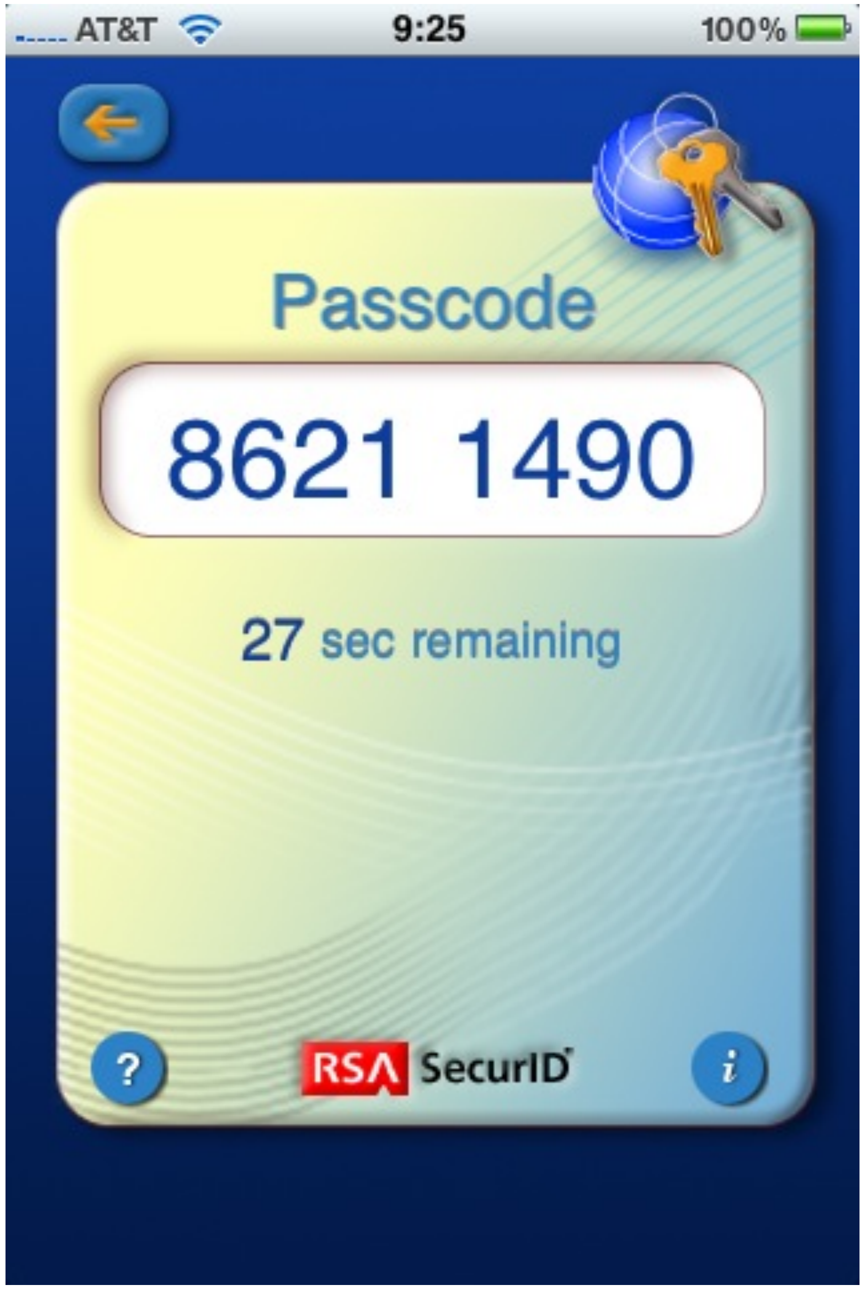
```
RISC/os (inet)

Authentication Server.

Id? ches
Enter response code for 70202: 04432234


Destination? cetus
$
```

SecureID

RSA Softkey



Enter PIN



Passcode

8621 1490

27 sec remaining

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

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**

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?

Better Solutions

#2: Limiting guesses

Limiting guesses

- **This has worked for ATM PINs since the early 1970s!**
- **It requires and authentication server, or some means to shut off the card/account**
- **It replaces the *eye of newt* rules with...**

An Engineering Goal: Non-moronic password rule!

Pick something a friend, colleague won’t guess in a few tries, and they can’t figure out while watching you type it

Summary solution

- Limited guesses and lock the account
- Non-moronic passwords
- Make locked accounts less painful

Grandma can understand and comply with this rule

- It makes sense
- Now, dictionary words are okay
- Simpler passwords are easier to remember
- You probably don’t have to write them down

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

We need research on account locking

- Not studied much in the open literature
- Practitioners could contribute:
  - what does a lost password cost?
  - how long will a user wait for an unlock?

Better Solutions?

#3: Grasping the “passphrase” nettle

Still Want Your Strong Passwords?

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

A Very Short Course on Work Factor

2^{10} = 1024 of the most common British words

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Pick one at random, entropy = 10 bits (2^{10} = 1024)

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what
will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people
know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good
back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might
day yes however put world over another in want as life most against again never under old much something why each while house part number out off different
went really thought came used children always four where without give few within about system local place great during although small before look next when
case end things social most find group quite mean five party every company women says important took much men information per both national often seen
given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long
hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young
council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market
towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today
mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health
turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself
themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear
staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea
whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting
church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street
home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language
land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role
true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value
member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank
countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong
situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground
conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed
cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach
lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for
happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine
letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis
whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities
provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving
normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director
prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy
consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association
nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate
husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear
investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed
appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay
needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish
opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference
operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional
easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier
title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through
glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Two random choices = 20 bits

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

20 bits = 2^{20} = 1,048,576

- “example early”
- to guess our two words, requires:
  - 1,048,576/2 guess, on average
- 6 random words would be 2^{60}
  - 1.15 x 10^{18}
- 8 random words gives you Avogadro’s number, a mole of work to do!

Good stuff!

- The list of words isn’t secret
- so spelling checker is okay!
  - so is error correction! In a password!
- easy words to type
- on an iPhone, pick words where the “tappos” give the word you wanted

Required entropy, according to Florêncio and Herley

- Facebook, Twitter, etc. are a minimum of ~20 bits
- Banks are in the 30s
- Government in the mid 40s and up

iPhone-Friendly?
(40 bits)

- grade likes jokes guess
- goes joke gold gods rode fire rows
- votes mines bored alike yard
- what knit bomb unit star grow
- actor agent above angel abuse
- honey learn least lemon links

www.cheswick.com/ches/insults.html

```
You grim-faced pipe of pleuritic snipe sweat
You dire chiffonier of foul miniature poodle squirt
You teratic theca of pathogenic moth dingleberry
You worrying pan broiler of bilious puff adder slobber
You vile wok of tumorigenic aphid leftovers
You baneful reliquary of pneumonic miller stumps
You atrocious terrine of harmful Virginia deer vomition
You excruciating pony of septic redstart eccrisis
You blotted kibble of unhygenic wild sheep spittle
You hard-featured fistula of podagric macaque flux
```

If you must, each line has 60 bits of entropy

- **value part peter sense some computer**
- **anxiety materials preparation sample experimental**
- **bliss rubbery uncial Irish**
- **2e3059156c9e378**
- **Gz4jgzkdxh**

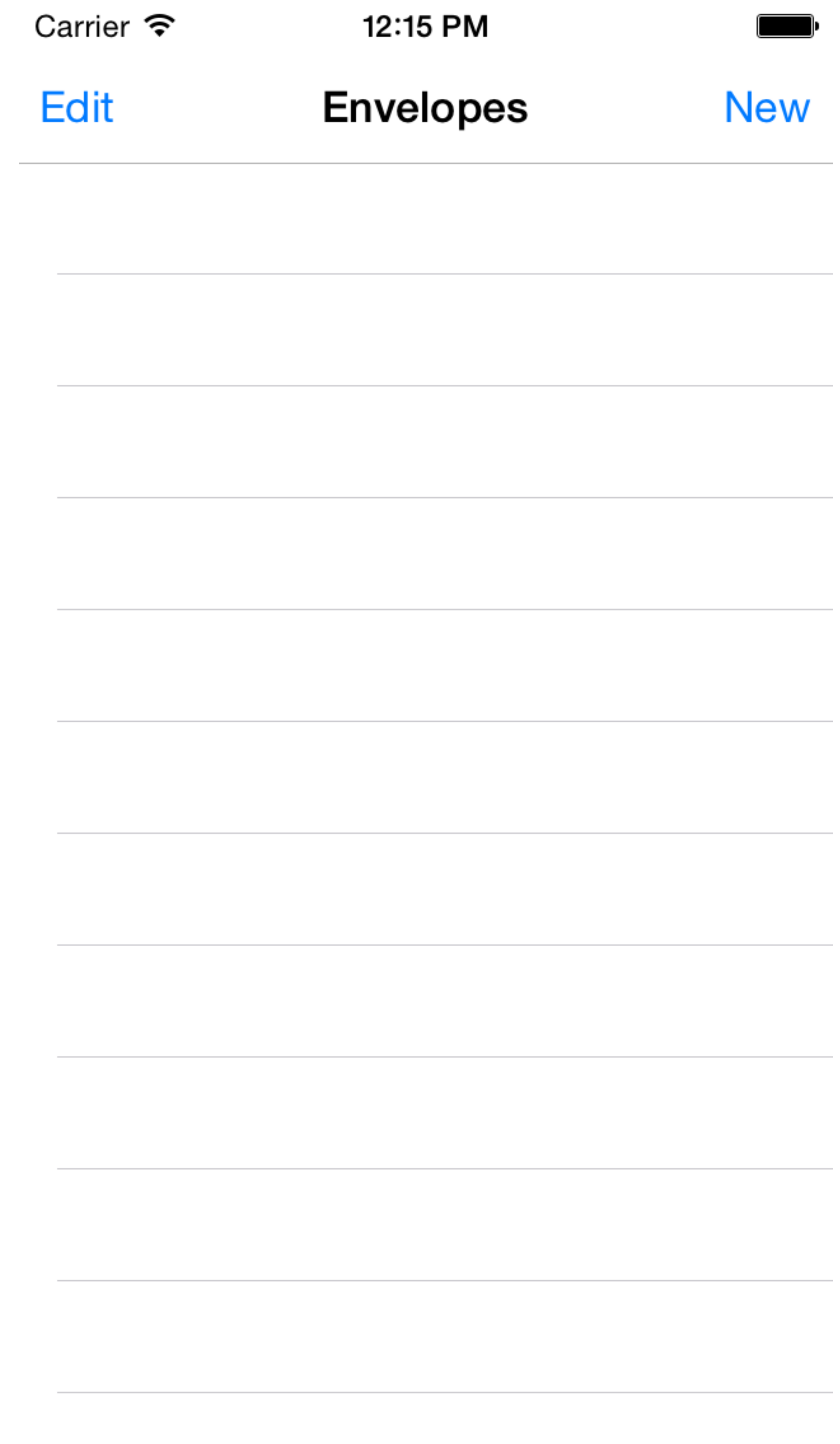
Dictionary attacks still a concern

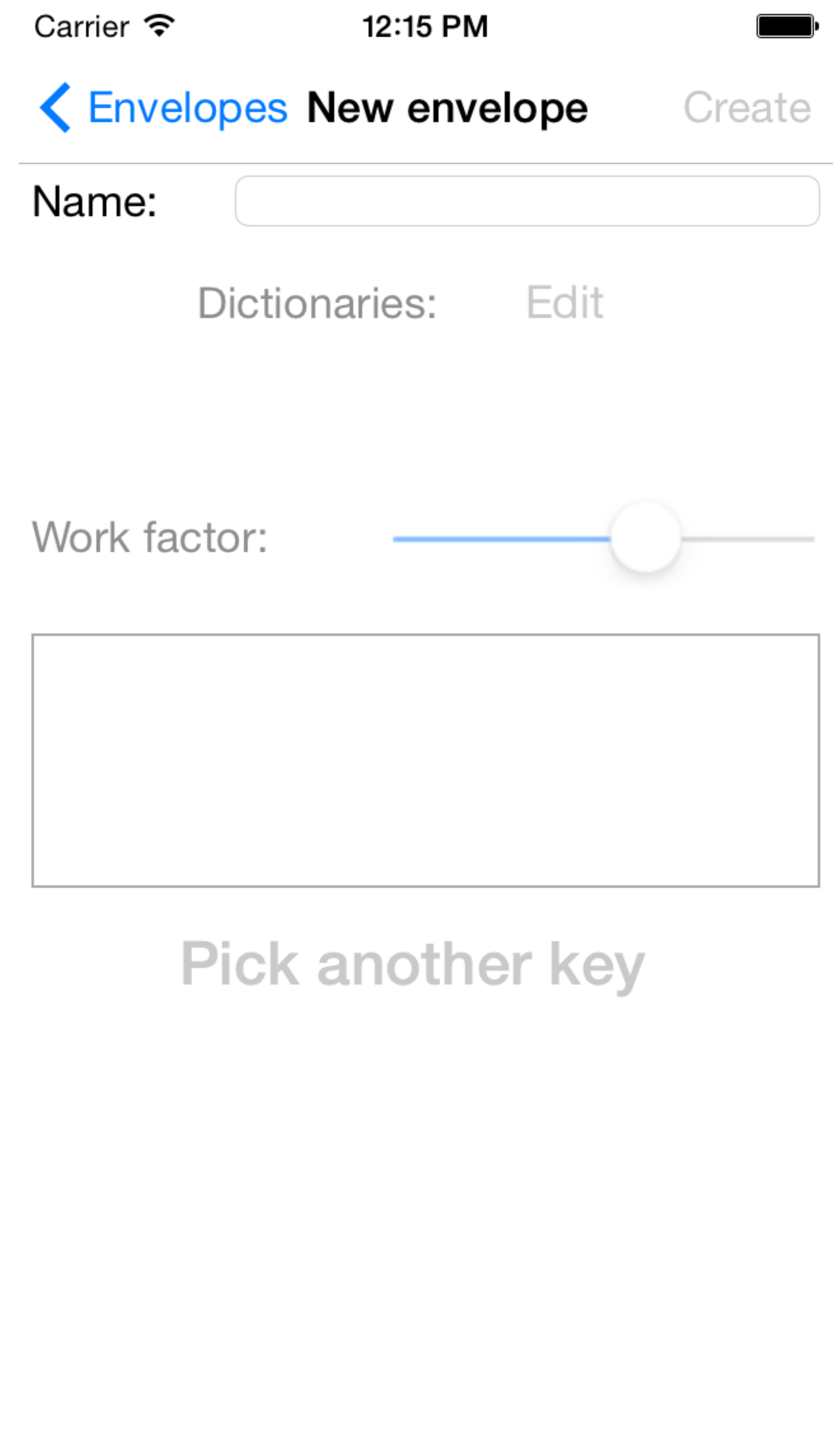
- **For standard Unix logins**
- **For ssh password logins**
- **Against captured oracle streams, like PGP and ssh key files, cleartext challenge/ response fields in protocols**
- **These are not mainstream attacks these days. Stolen laptops/iPhones a concern**

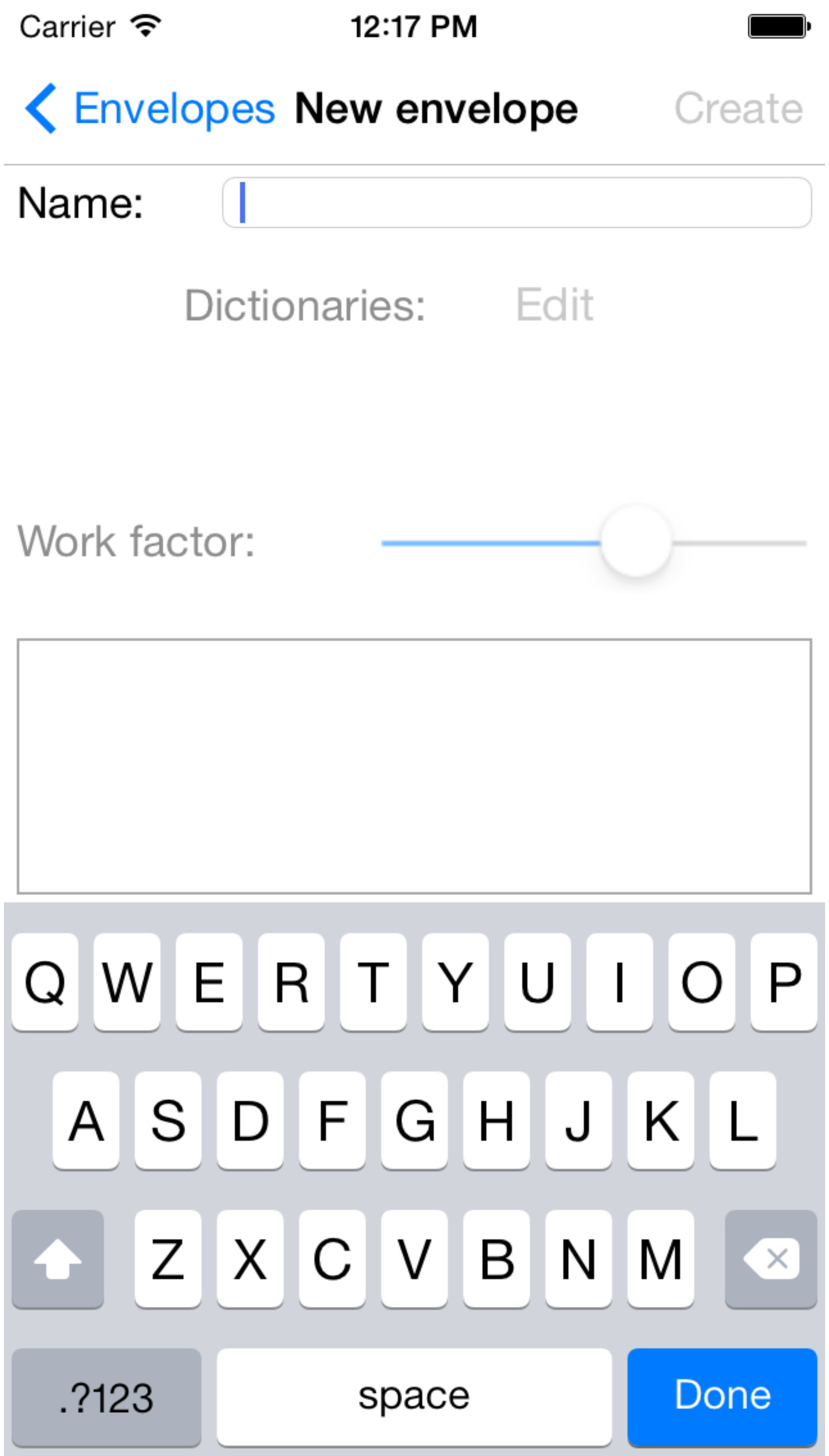
If you really need “high entropy” passwords

- 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?

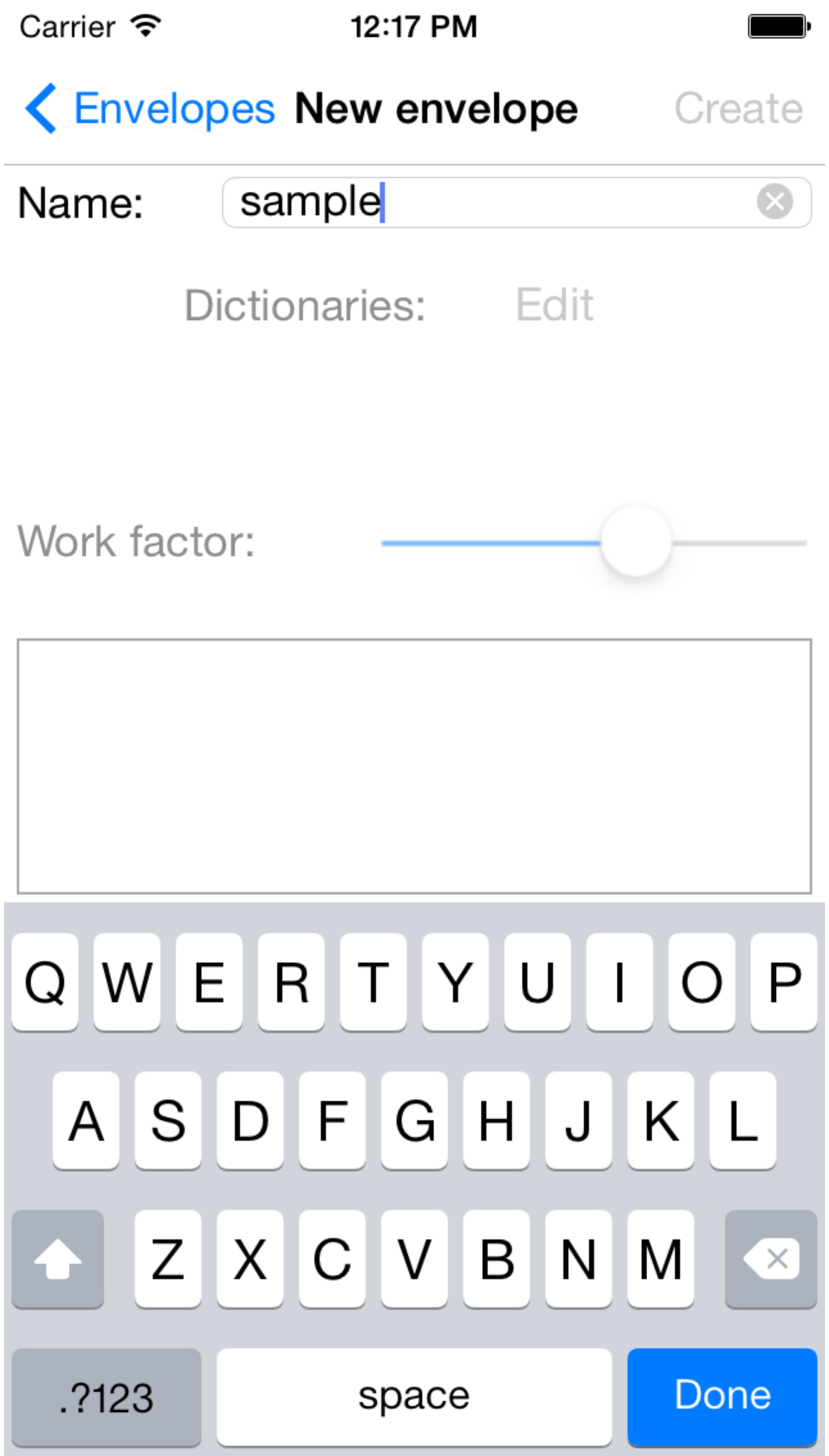
(105 demo)


Carrier
12:15 PM
Edit
Envelopes
New

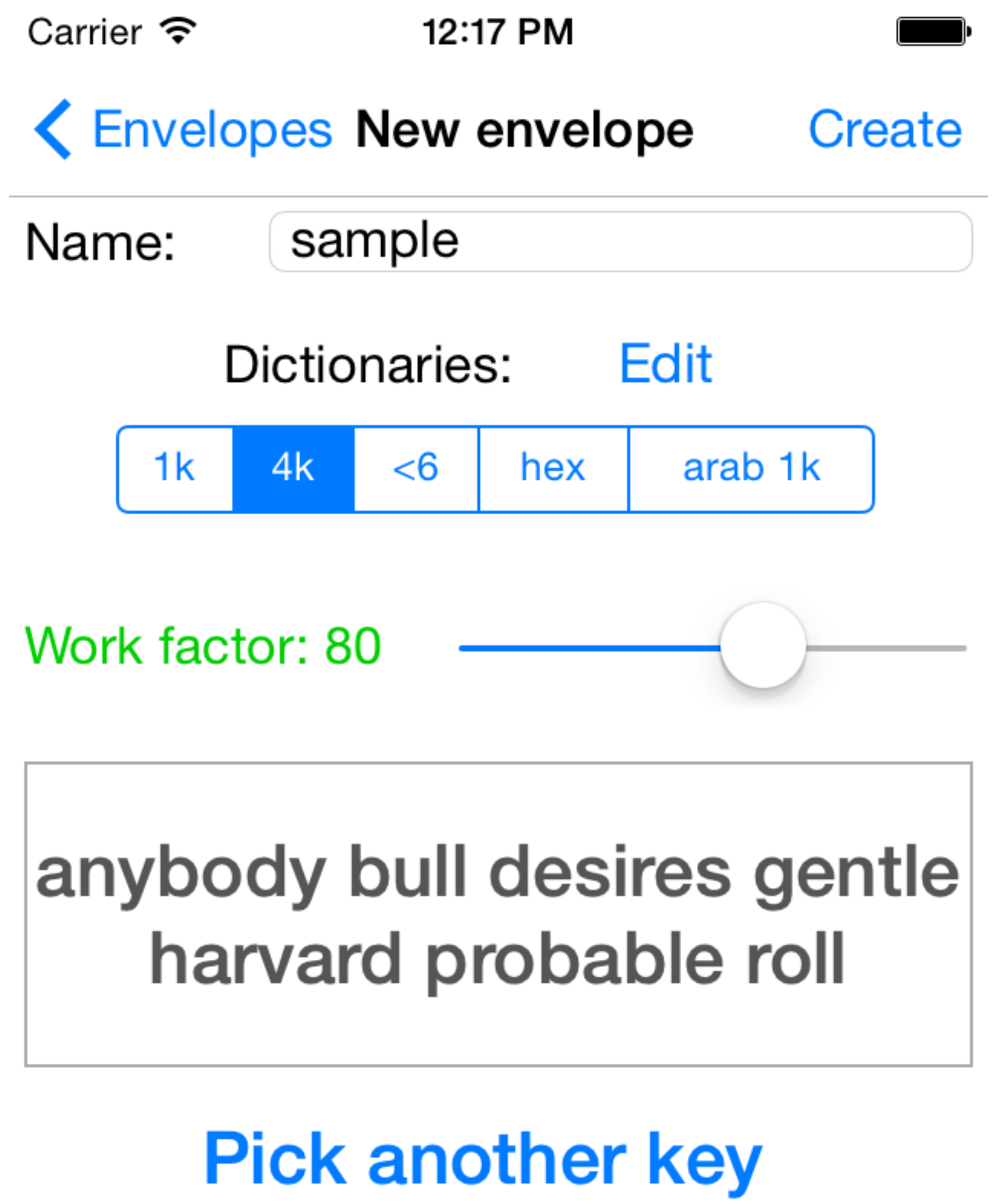

Carrier
12:15 PM
Envelopes
New envelope
Create
Name:
Dictionaries:
Edit
Work factor:
Pick another key



Name:



Name: sample



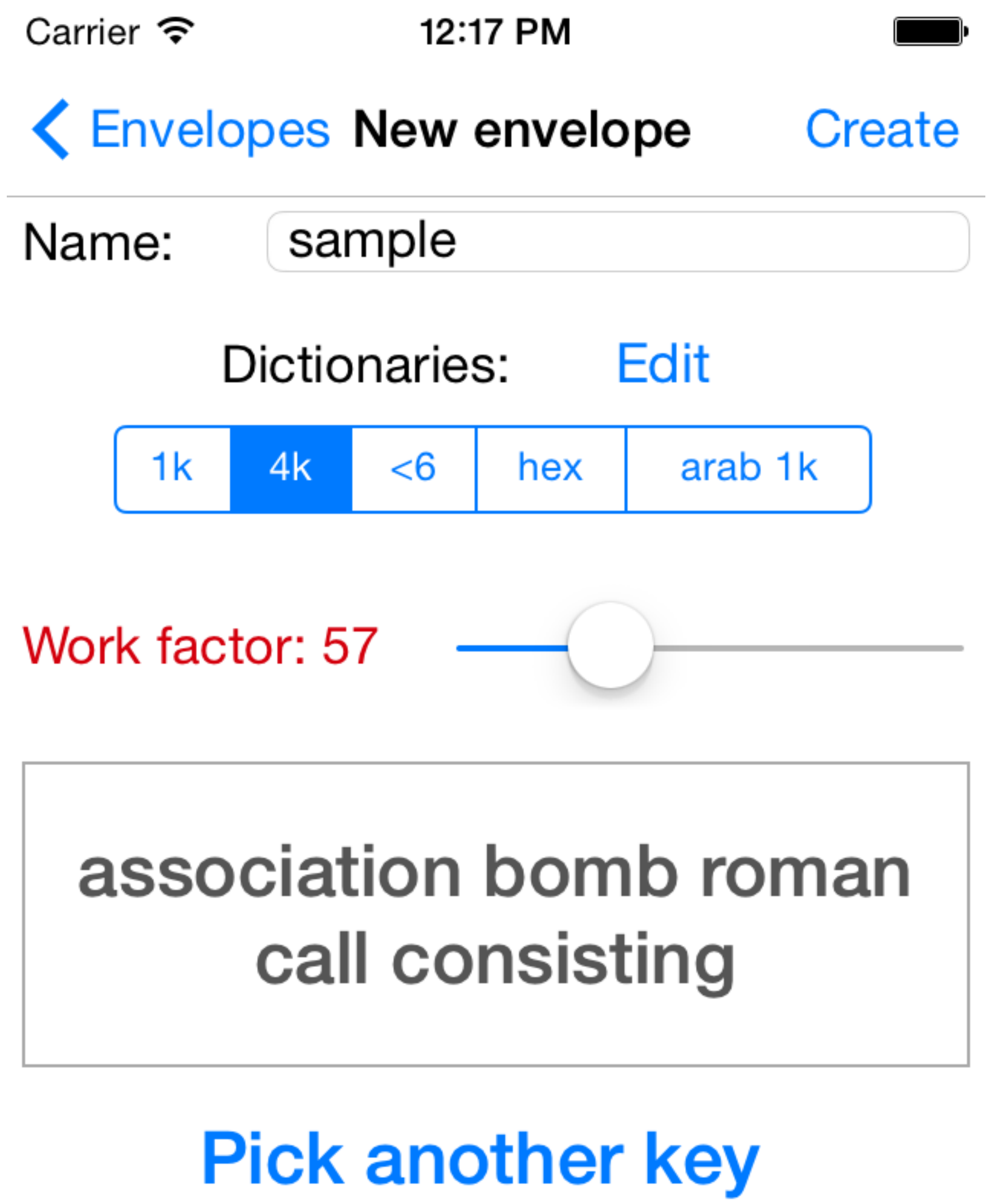
New envelope

Name: sample

Dictionaries: 4k

Work factor: 80

anybody bull desires gentle harvard probable roll



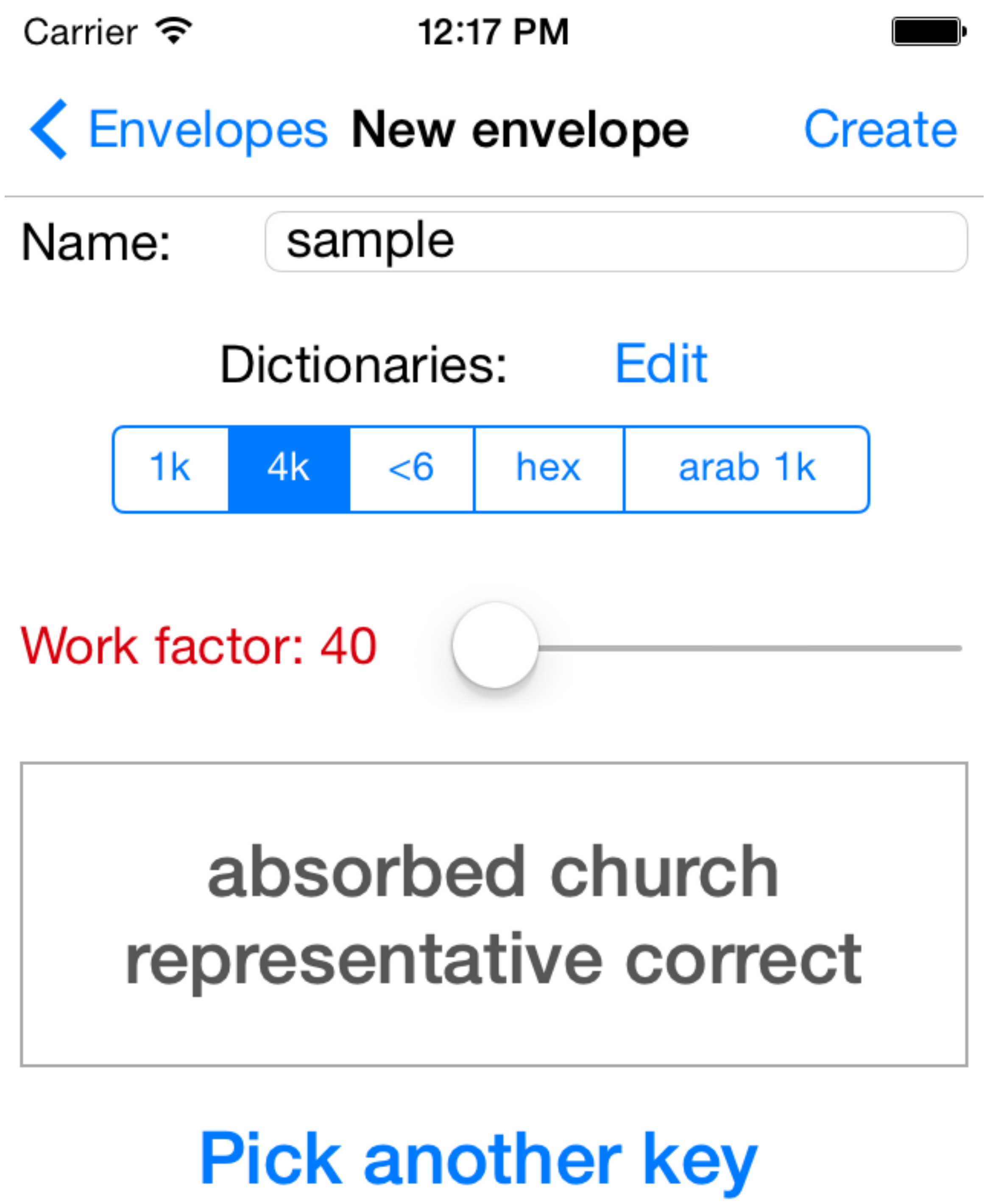
New envelope

Name: sample

Dictionaries: 4k

Work factor: 57

association bomb roman call consisting

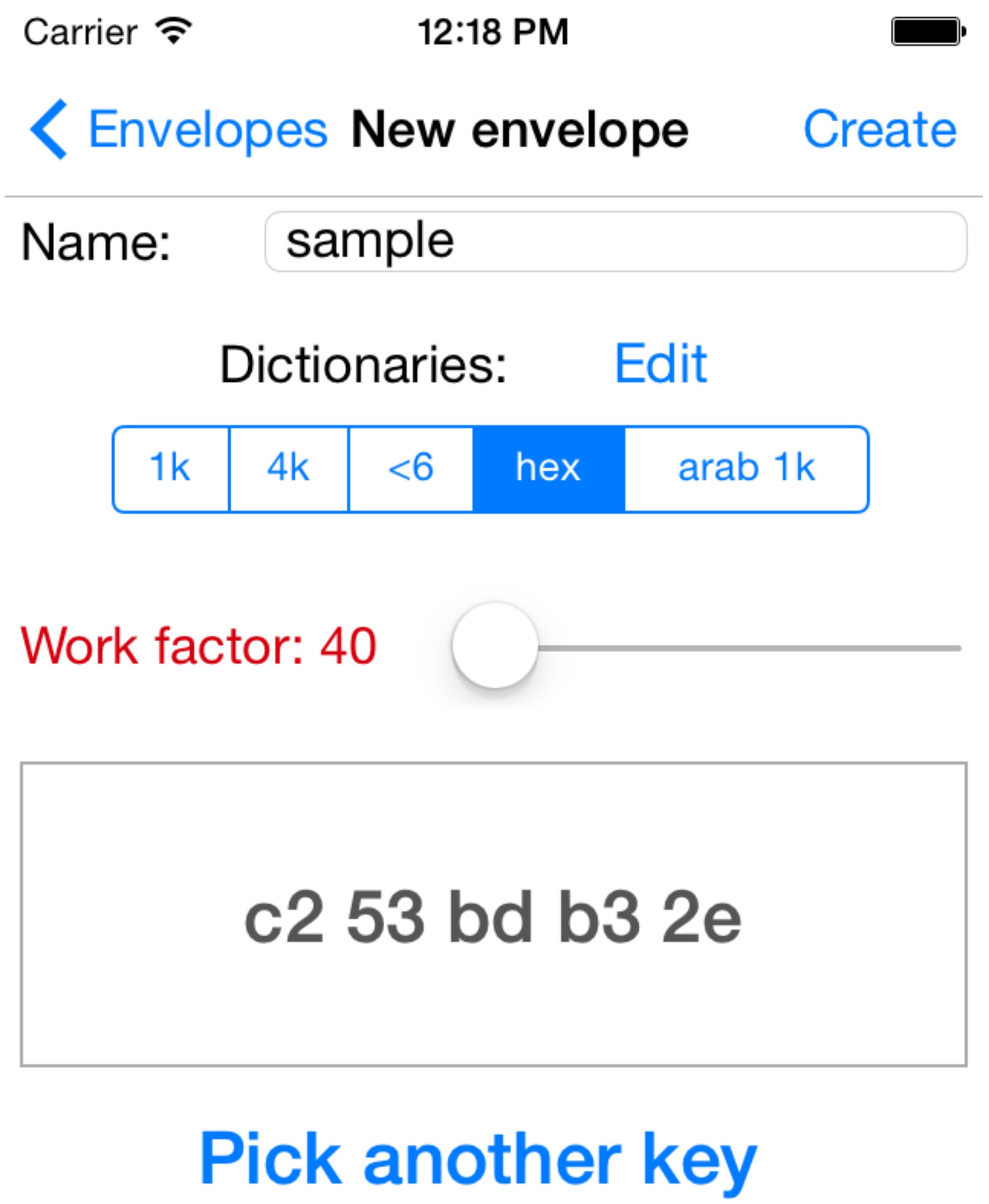


Name: sample

Dictionary: 4k

Work factor: 40

absorbed church representative correct

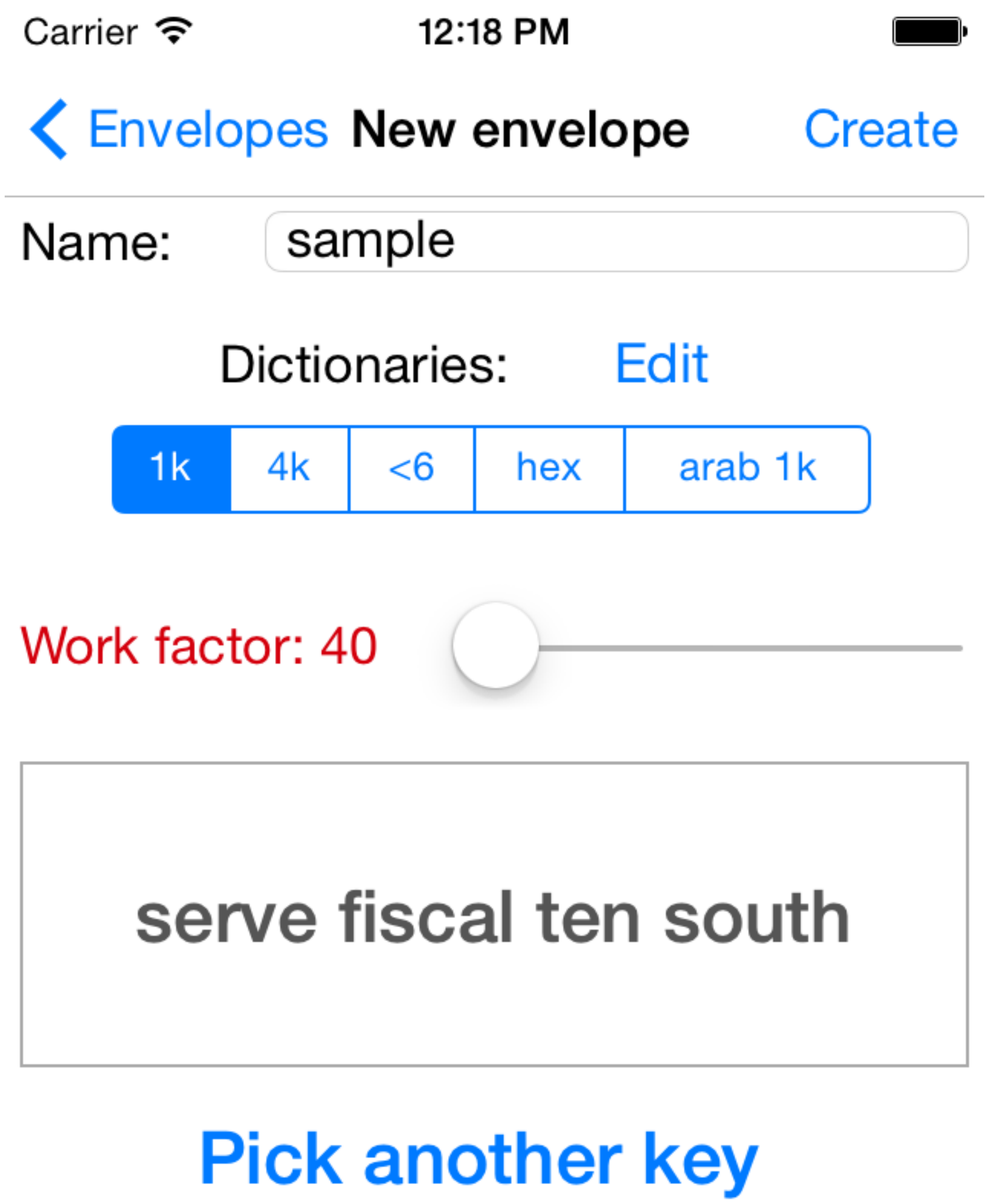


Name: sample

Dictionary: hex

Work factor: 40

c2 53 bd b3 2e

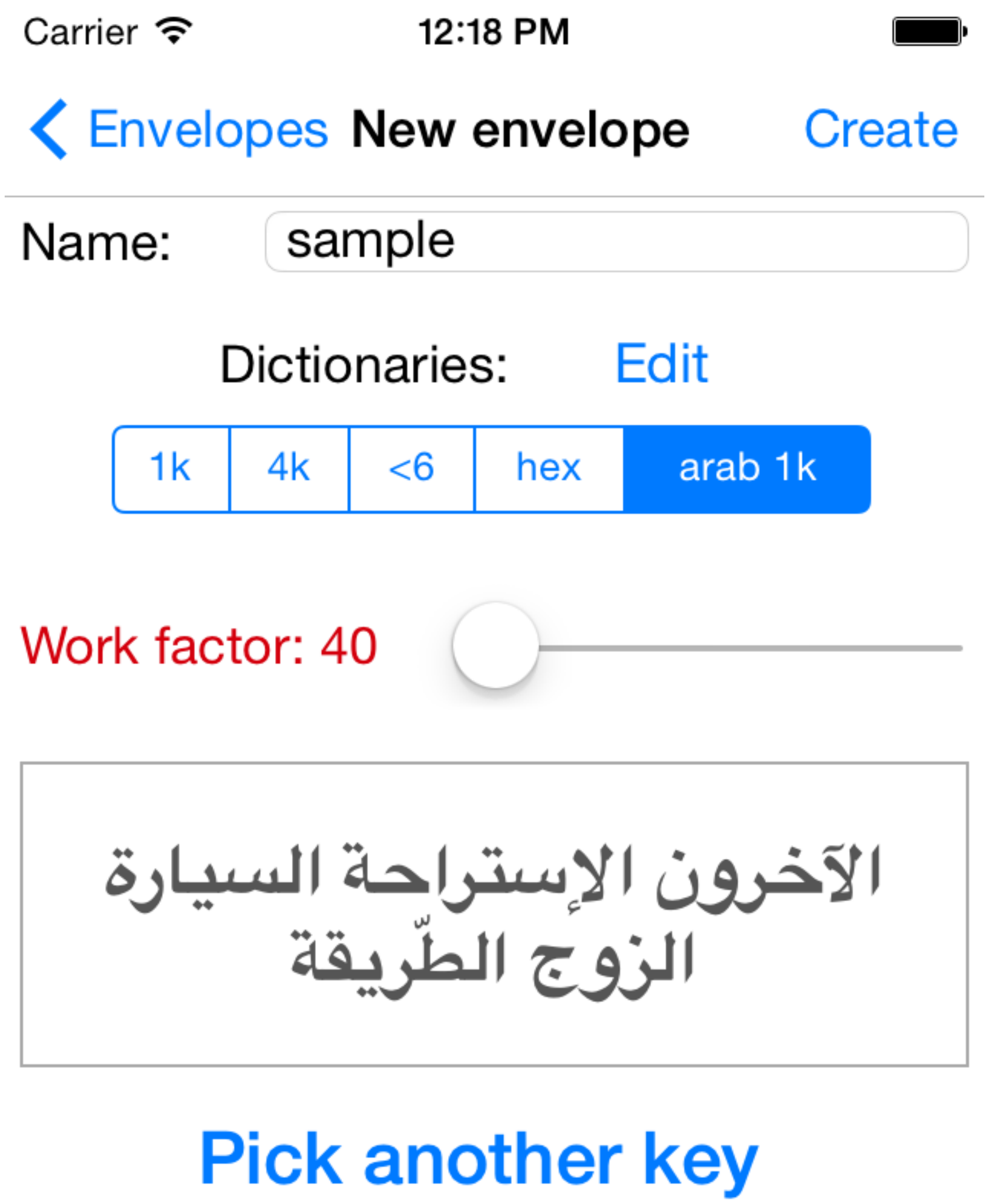


Name: sample

Dictionaries: 1k

Work factor: 40

serve fiscal ten south

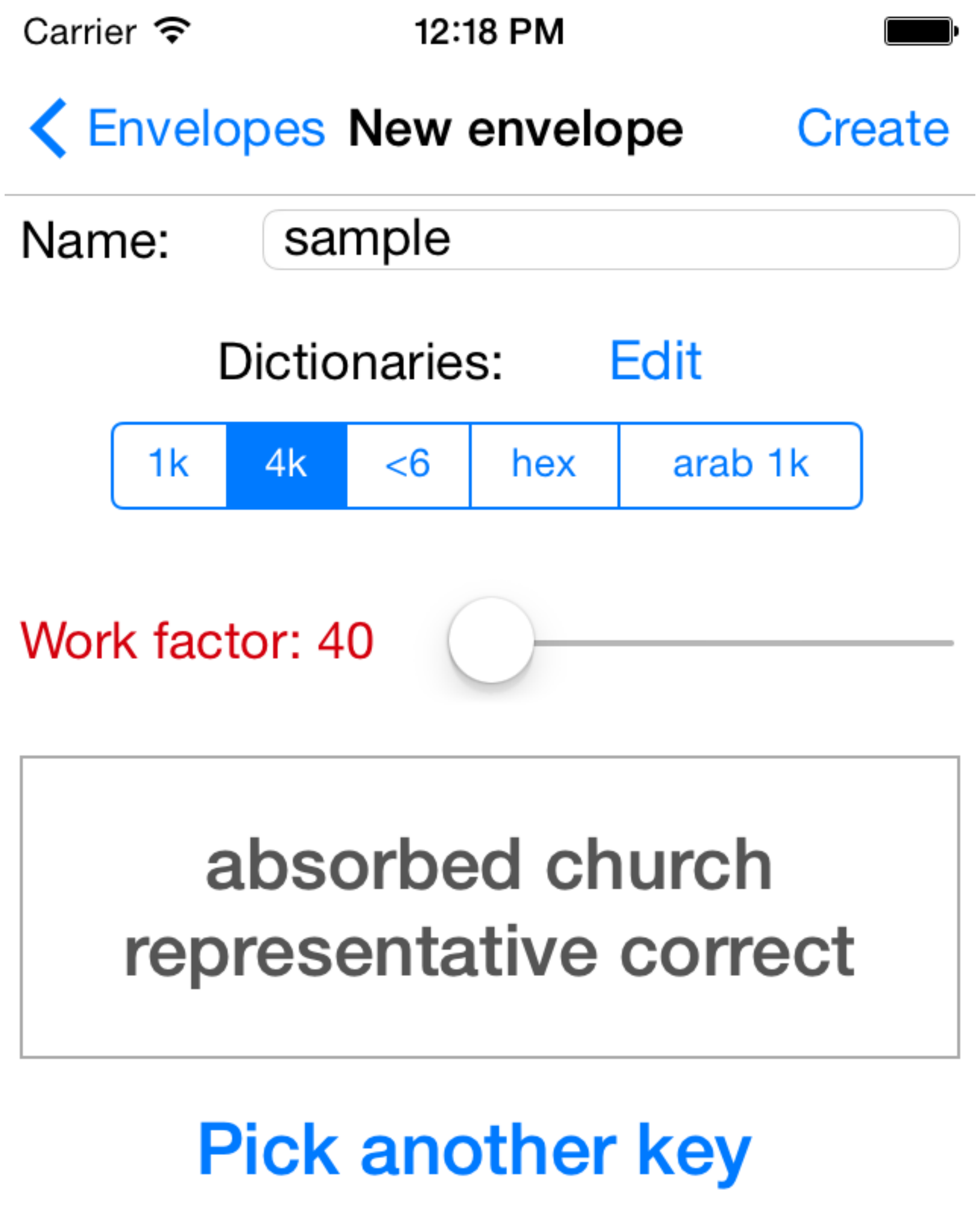


Name: sample

Dictionaries: arab 1k

Work factor: 40

الآخرون الإستراحة السيارة
الزوج الطّريقة

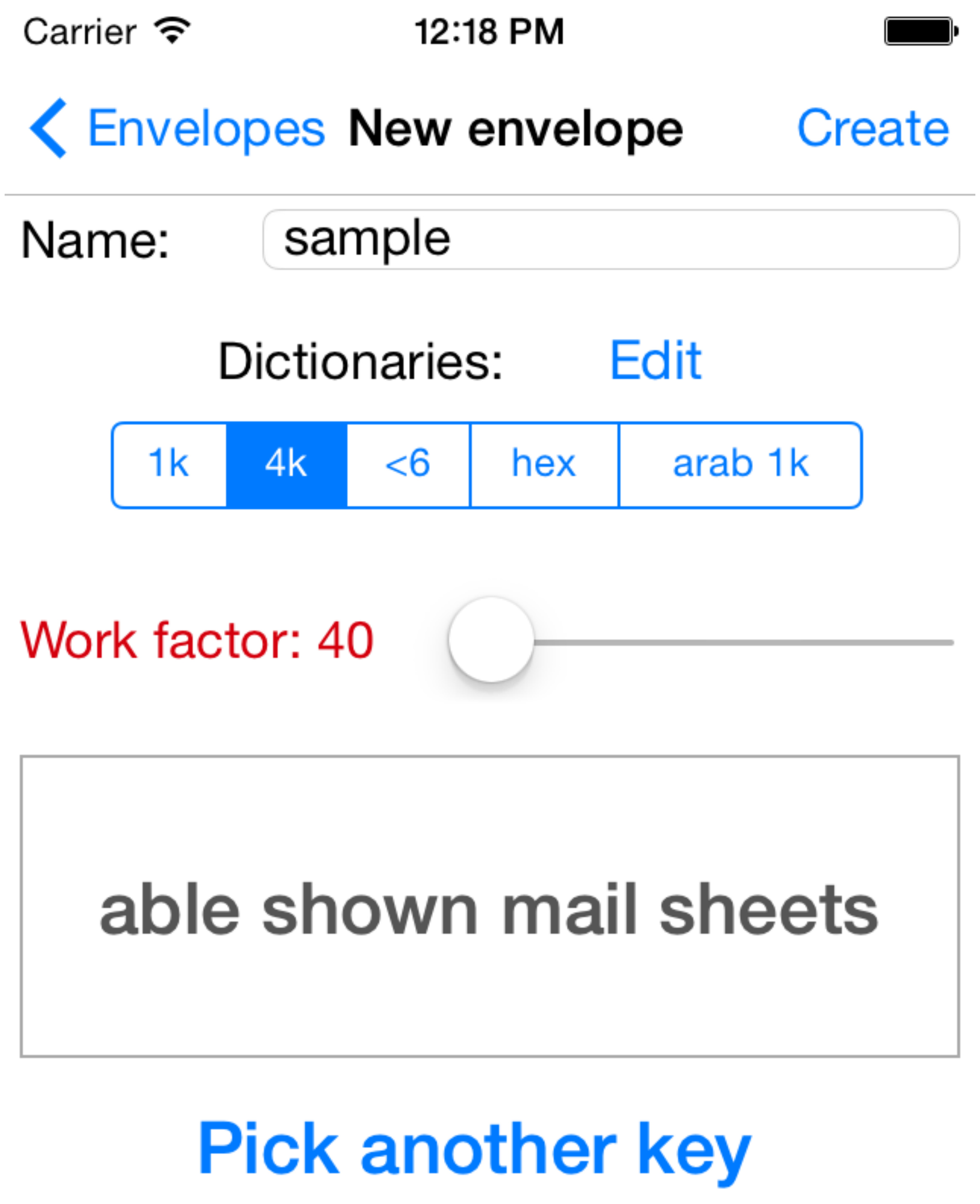


Name: sample

Dictionaries:

Work factor: 40

absorbed church representative correct

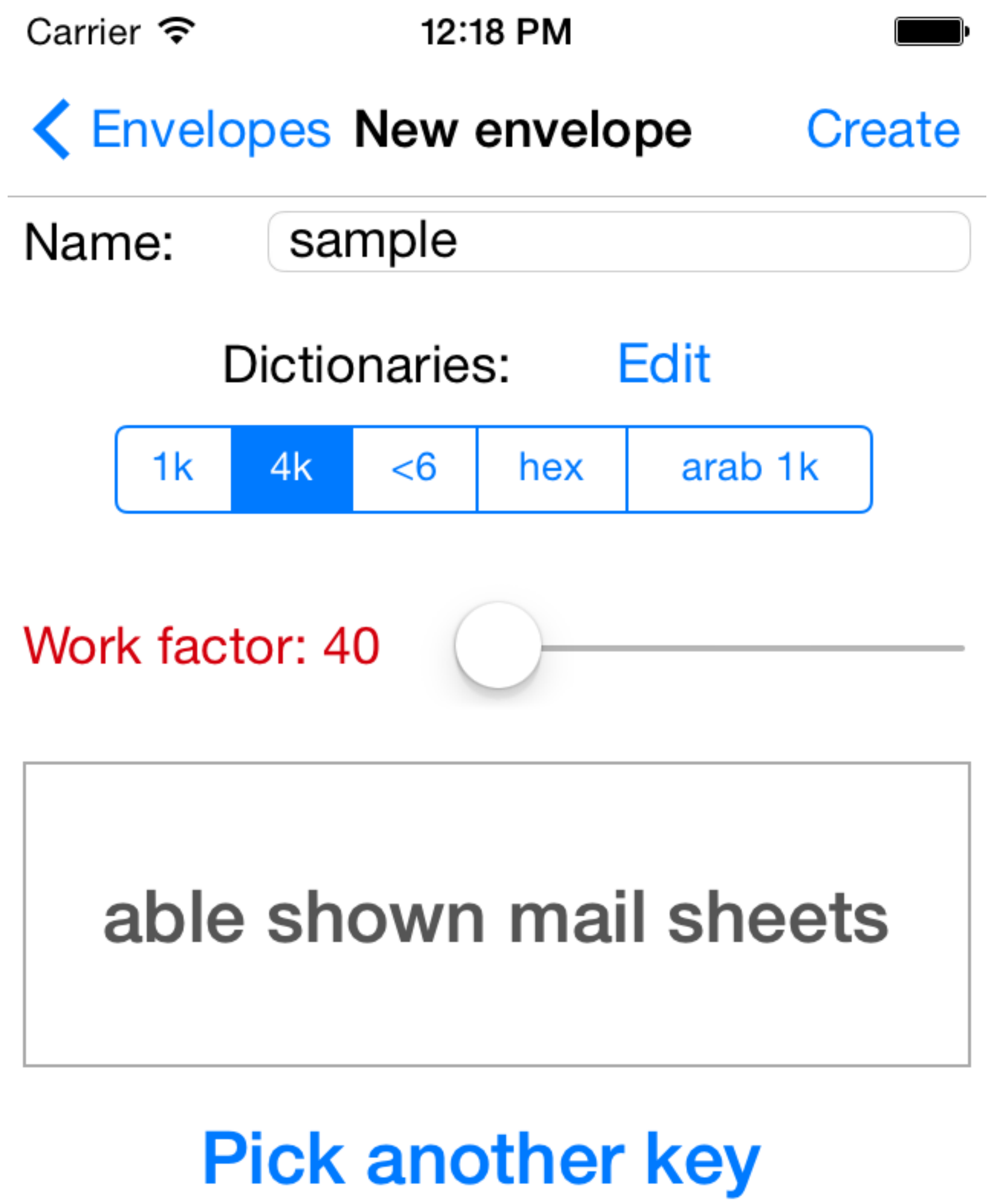


Name: sample

Dictionaries:

Work factor: 40

able shown mail sheets

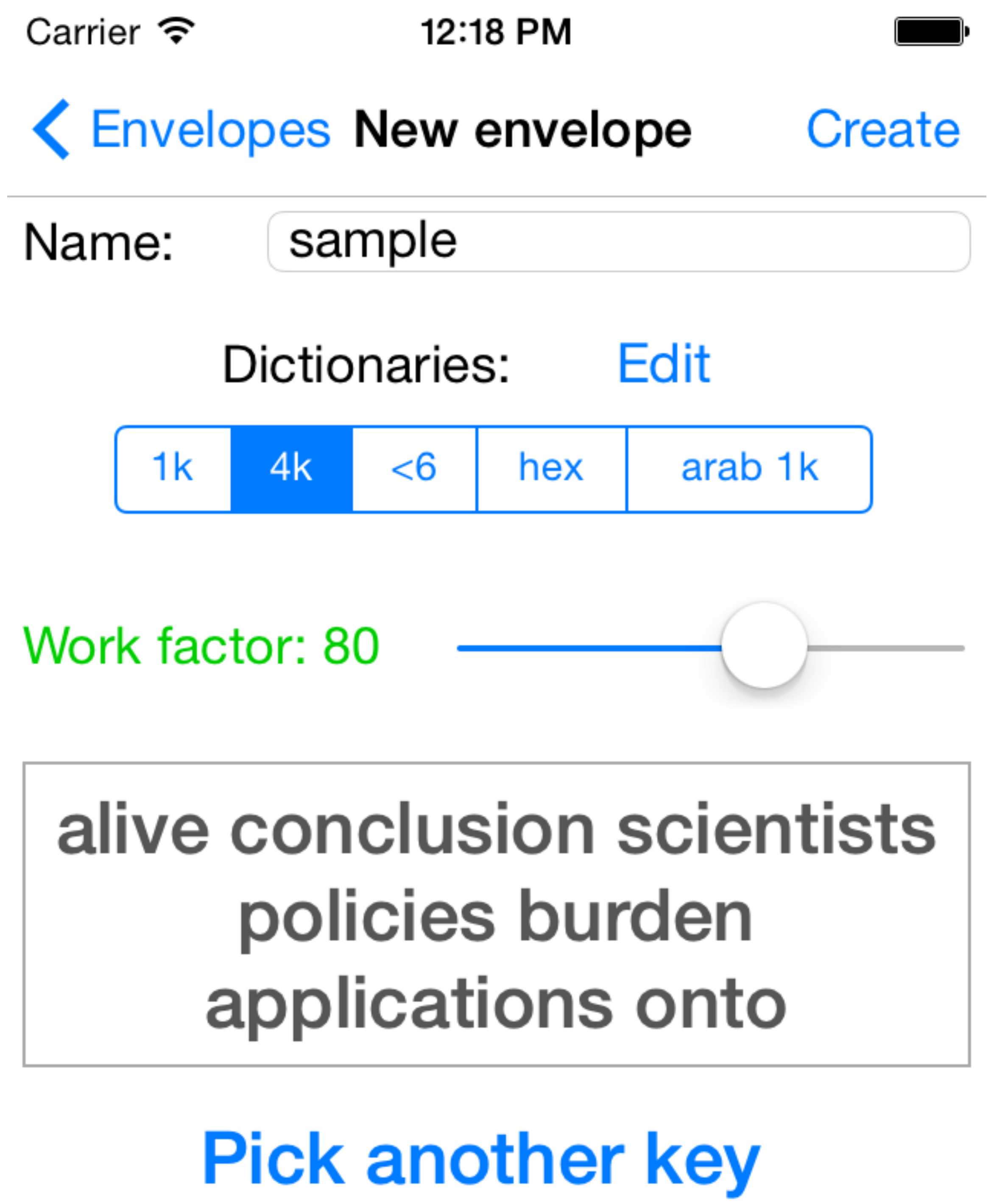


Name: sample

Dictionaries: 4k

Work factor: 40

able shown mail sheets

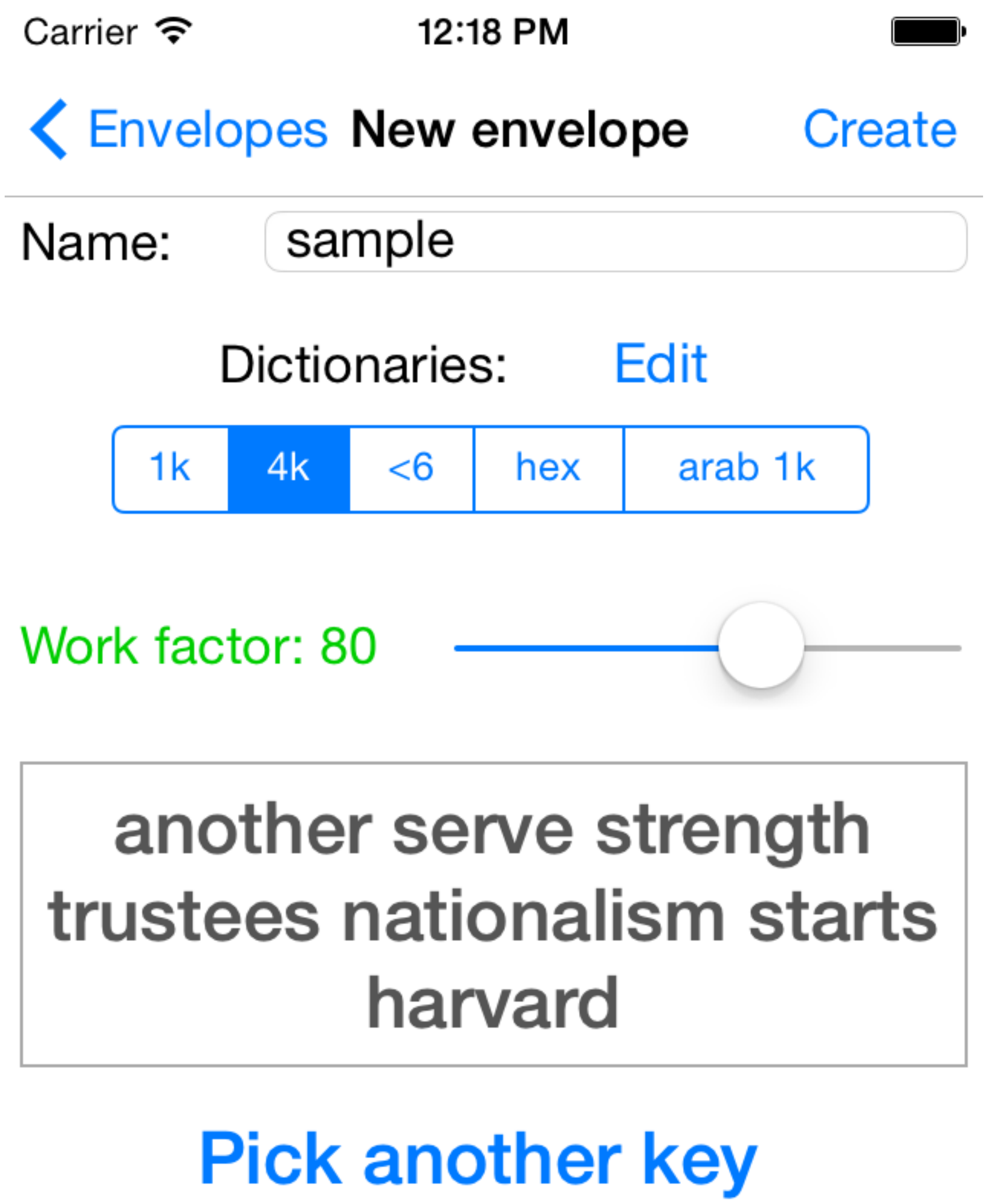


Name: sample

Dictionaries: 4k

Work factor: 80

alive conclusion scientists policies burden applications onto

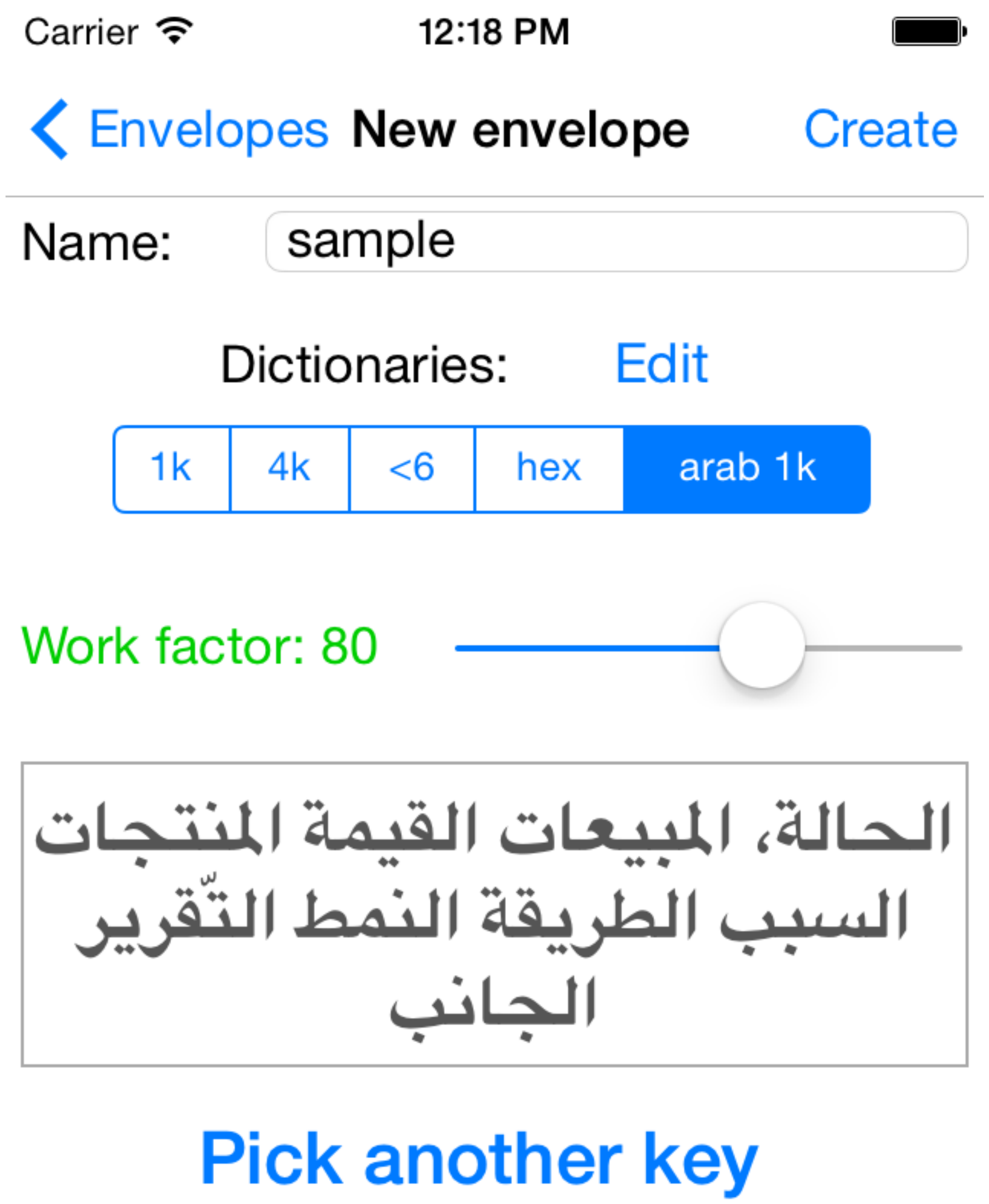


Name: sample

Dictionaries:

Work factor: 80

another serve strength trustees nationalism starts harvard



Name: sample

Dictionaries:

Work factor: 80

الحالة، المبيعات القيمة المنتجات
السبب الطريقة النمط التّقرير
الجانب

Use one Really Strong password to lock your password wallet

- **You are not going to remember it immediately**
- **You will learn it after a while**
- **You don’t have to change it**
- **2^105 bits means average work factor of 20,282,409,603,651,670,423,947,251,286,016 =**
- **20 * 10^30 = 33 million times Avogadro’s number**

Benefits

- The dictionary is not secret
- You can use spelling checkers
- No fancy-pants attacks by Dave Wagner or anyone else
- The wallet can be stored in a public place, or even on your smart phone and backups
- You can lose your smartphone without leaking secrets from the wallet
- One can build authentication into this, giving challenge/response

Of course, there are a lot of assumptions here

- Secure client software
- No shoulder surfing
- Your written backup could fall in the wrong hands
- Rubber hose cryptography
- Wallet software could leave useful traces behind in the smart phone
- ….

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

Updated Advice

For Implementors

Out of the Dictionary Attack Game Game

- Count and manage authentication attempts with a server
- pam_tally
- slow or block accounts (block is better than loss of control of an account)
- blacklist inquisitive IP addresses
- Avoid strong passwords in most cases

Implement security where Don’t Be a Moron is good enough

- **Any character is legal, except newline and backspace**

Use an authentication server

- **Centralizes the security function**
- **Make it strong and robust**
- **Replication is dangerous, reliability is better**
- **Limit authentication attempts**
- ***DO NOT LET IT BE COMPROMISED***

Near-public authentication servers

- **OpenID**
- **Openauth**
- **The general idea is appealing**

Identify the auth. server and pw rules

- Usually just an additional line to a web pages
- Yes, it leaks a little information
- It greatly eases the usability
  - name of server eliminates guessing and pw leakage
  - rules remind user of pw variation used

Don’t make acct. names too easy to guess

- Thwarts single password, multi-account scans
- U.S. Social security numbers are a little too guessable. Credit cards seem to be okay.
- But secret rules (hyphens in social security number?) reduce usability without improving security

PIN != password

- **A PIN is a sequence of digits only**
- **A password is a superset of PINs**
- **A passphrase is a series of words, but probably should not be called a *phrase*. *Passcode* is probably better**

Getting out of the game: ssh

- **disable password logins. Use DSA key from a trustable client, that key locked with a strong pass-phrase**
  - **two-factor authentication**
  - **dictionary attack is rare endgame: you have to steal or own the client first**
  - **Reasonably secure clients are doable**

Use Client certificates to limit attack surface

- Limiting connections to those with known client certificates gets you mostly out of the game
- Many mail clients do not offer client cert. processing, and should

Yeahbuttal

Yeahbuttal

- These ideas will take time to deploy, if they do
- Huge installed base
- Corporate conglomerates have hundreds or thousands of these!

Yeahbuttal

- Who owns the app?
- Who hosts it?
- Third party applications? (401k, health, etc.)
- Who developed it? (often long gone)
- What is the business function
- Buy-in is needed from all parties
- Development costs?

Fix it anyway

- This is one of those economies of scale you told the shareholders the merger was going to buy
- Authentication servers should be relatively simple to code and maintain
- If you don’t understand who your users are, your security is shot from the start

Fix it Anyway

- **Annoyed users are uncooperative users**
- **There is a substantial cost when a large community has to deal with authentication foolishness on a routine basis**

Strong Authentication, not strong passwords

- Use multi-factor authentication when it is really important
- Ubiquitous laptops and cell phones can be used for middle-level authentication

Selling weaker passwords

- **ATM PINs of 4 digits work fine**
- **Cut user support costs**
- **Backup passwords are usually weaker**
- **Improve the users' experience**
- **Annoyed users are less cooperative**
- ***Tell them I (#98!) said it was probably a good idea***

Summary

- Distribute and require client certificates
- Use ssh with pass-phrased locked digital key, never passwords
- Use crypto services, like IMAPS, SMTPS
- Limit password attempts

Frankly, I am sick of this!

Several solutions that work

Current threats vs. better passwords

- Keystroke loggers
  - needs strong, reliable clients. OS!
- Phishing attacks
  - some usability hacks would help
- Password database compromise
  - up to the pros. Need stiffer sentences.

People, we have to do better than this

- The Bad Guys are getting much better
- Our computer systems are getting much more important to us
- Security has to be thought about, and reviewed

Dangerous browsing

- ***All Your IFRAMES Point to Us*, Provos and Mavrommatis (Google), Rajab and Monrose (JHU); Usenix Security 2008**

Dangerous patches

- ***Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications.*** **Brumley and Poosankam (CMU), Song (Berkeley), Zheng (Pitt); Proceedings of the IEEE Security and Privacy Symposium, May 2008.**

Provably-hidden malware

- ***Analysis-Resistant Malware.*** **Bethencourt and Song (BSD/CMU), Waters (SRI). ISOC NDSS, Feb 2008.**

COTS CPUs dangerous?

- ***Designing and Implementing Malicious Hardware.*** **King, Tucek, Cozzie, Grier, Jiang, and Zhou (U Illinois at Urbana Champaign). Usenix LEET 2008, April, San Francisco.**

Stuxnet

- **The pros are *very* good at this sort of thing**

Rethinking Passwords

Bill Cheswick
ches@cheswick.com
Visiting scholar, U. Penn.