CS5438
Security and Privacy: Practice and Case Studies

$c = m^e \bmod n$

Passwords, or the "Weakest Link"
3 February 2016

Instructors: Ari Juels and Vitaly Shmatikov
Spring 2016

User authentication today is a mess.

The case of Mat Honan
3 August 2012

- 4:33 p.m., “Mat Honan” called AppleCare reporting lost me.com e-mail password. Apple issued temporary password.
  - “Mat” couldn’t answer his own security questions.
  - Apple required only last four digits of a credit card and a billing address.
- 4:50 p.m.: Password reset e-mail arrived in Honan’s me.com e-mail box; used to reset Honan’s AppleID password
- 4:52 p.m.: GMail password recovery e-mail arrived in Honan’s me.com mailbox
- 4:54 p.m.: Honan’s Google account password changed.

Matt Honan, *Wired* correspondent

The case of Mat Honan
3 August 2012

- 5:00 p.m.: iCloud “Find My” tool used to wipe Honan’s iPhone
- 5:02 p.m.: Honan’s Twitter password reset
- 5:05 p.m.: Honan’s MacBook wiped
- 5:10 p.m.: The *real* Honan calls AppleCare
- 5:12 p.m.: Hackers post message on Honan’s Twitter account taking credit for the hack

Matt Honan, *Wired* correspondent

How did it happen?

- Attackers started by compromising Honan's Amazon account
- Needed credit card number for Honan’s Amazon account. How did they learn it?
- Attackers called Amazon and **added** a new credit card number to Honan’s account. (Name, e-mail, and billing address sufficed.)
- Attackers called Amazon to reset Honan’s password. For identity verification, Amazon asked for a credit card number…

Matt Honan, *Wired* correspondent

How did it happen?

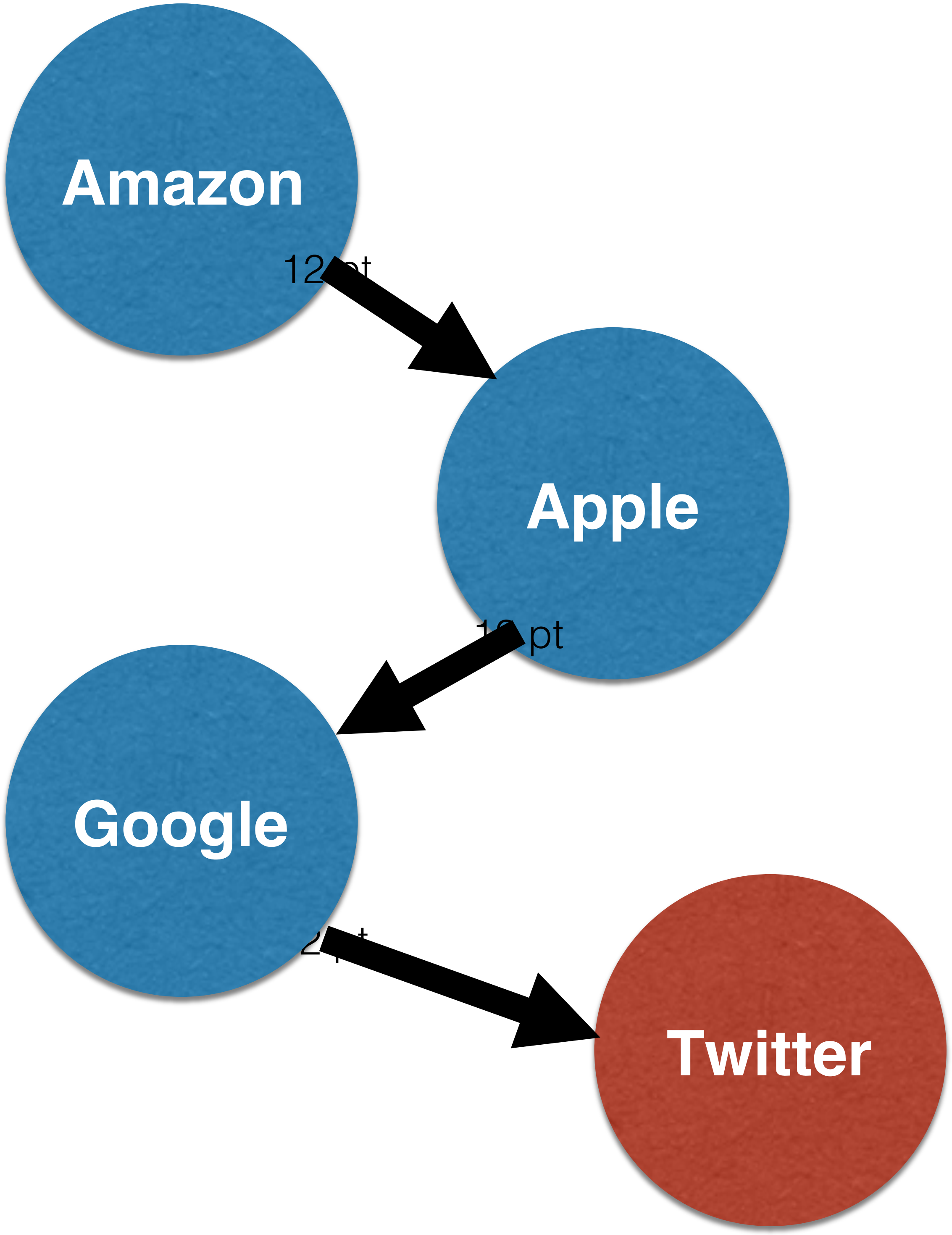
- Once logged in to Honan’s Amazon account, attackers learned last four digits of real credit card numbers
- “*The very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers security enough to perform identity verification.*”

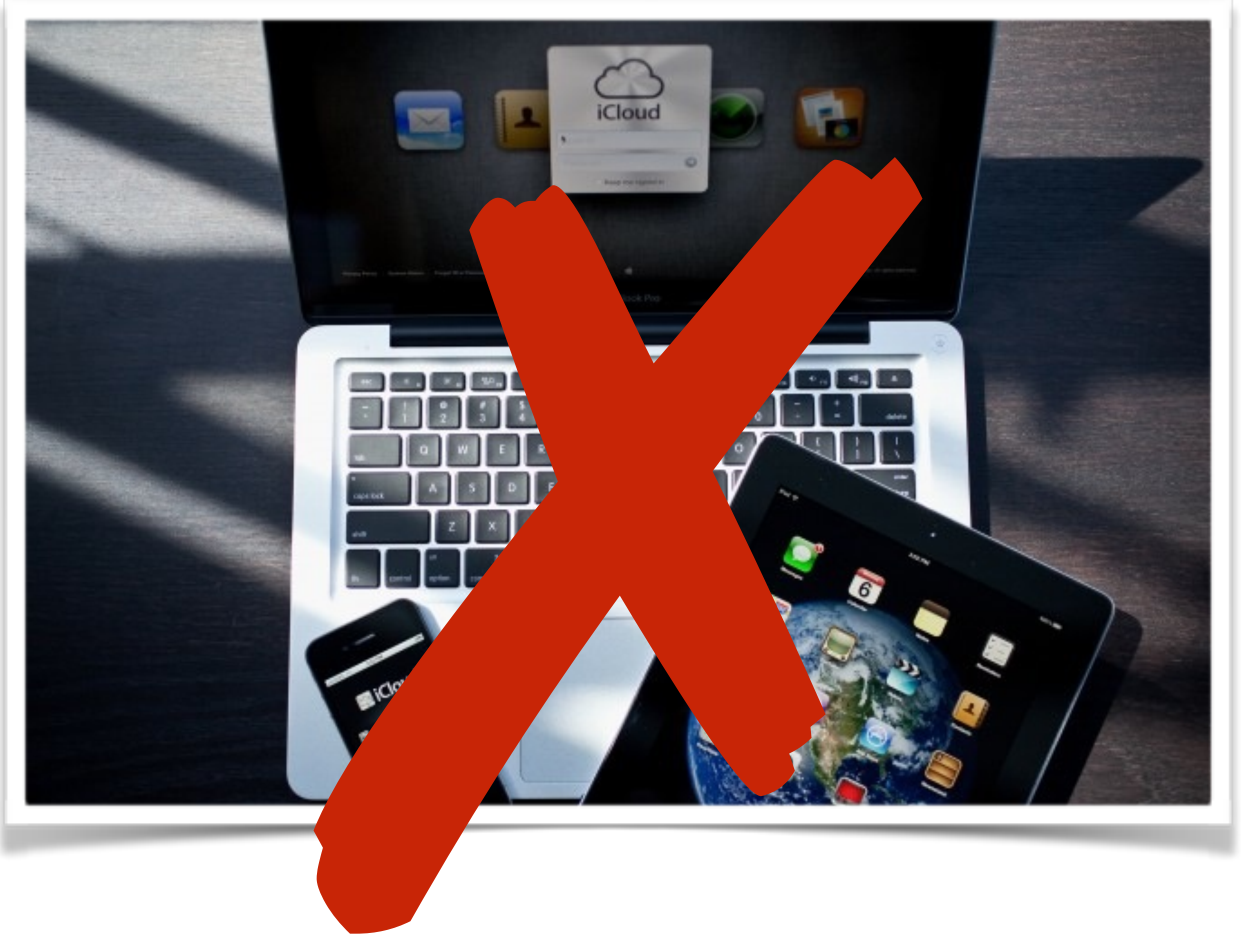
Matt Honan, *Wired* correspondent

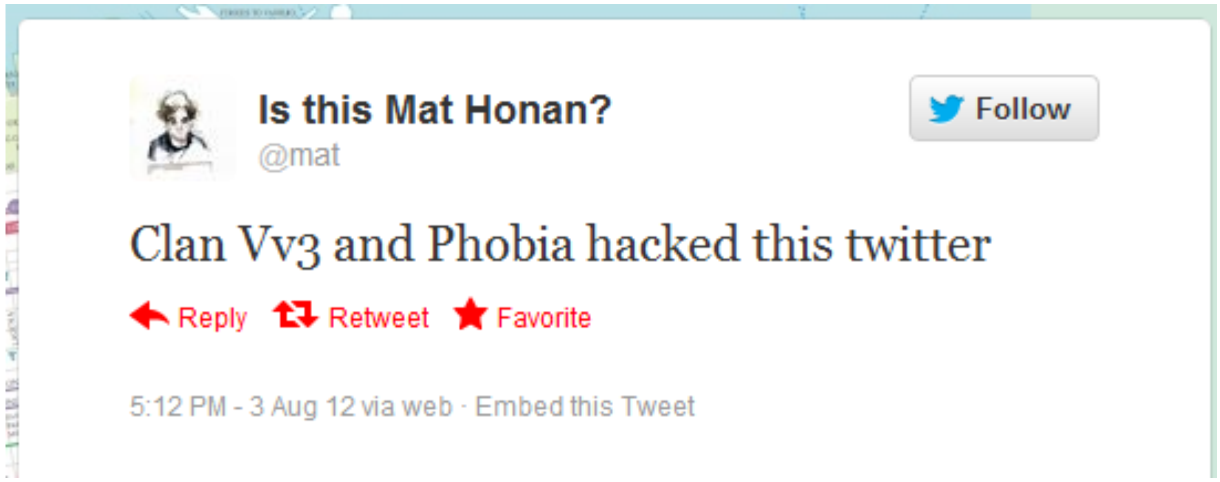
How did it happen?

- Then they called AppleCare…
- “*It turns out, a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account. Once supplied, Apple will issue a temporary password, and that password grants access to iCloud.*”

Recap







Is this Mat Honan?
@mat

Clan Vv3 and Phobia hacked this twitter

5:12 PM - 3 Aug 12 via web · Embed this Tweet

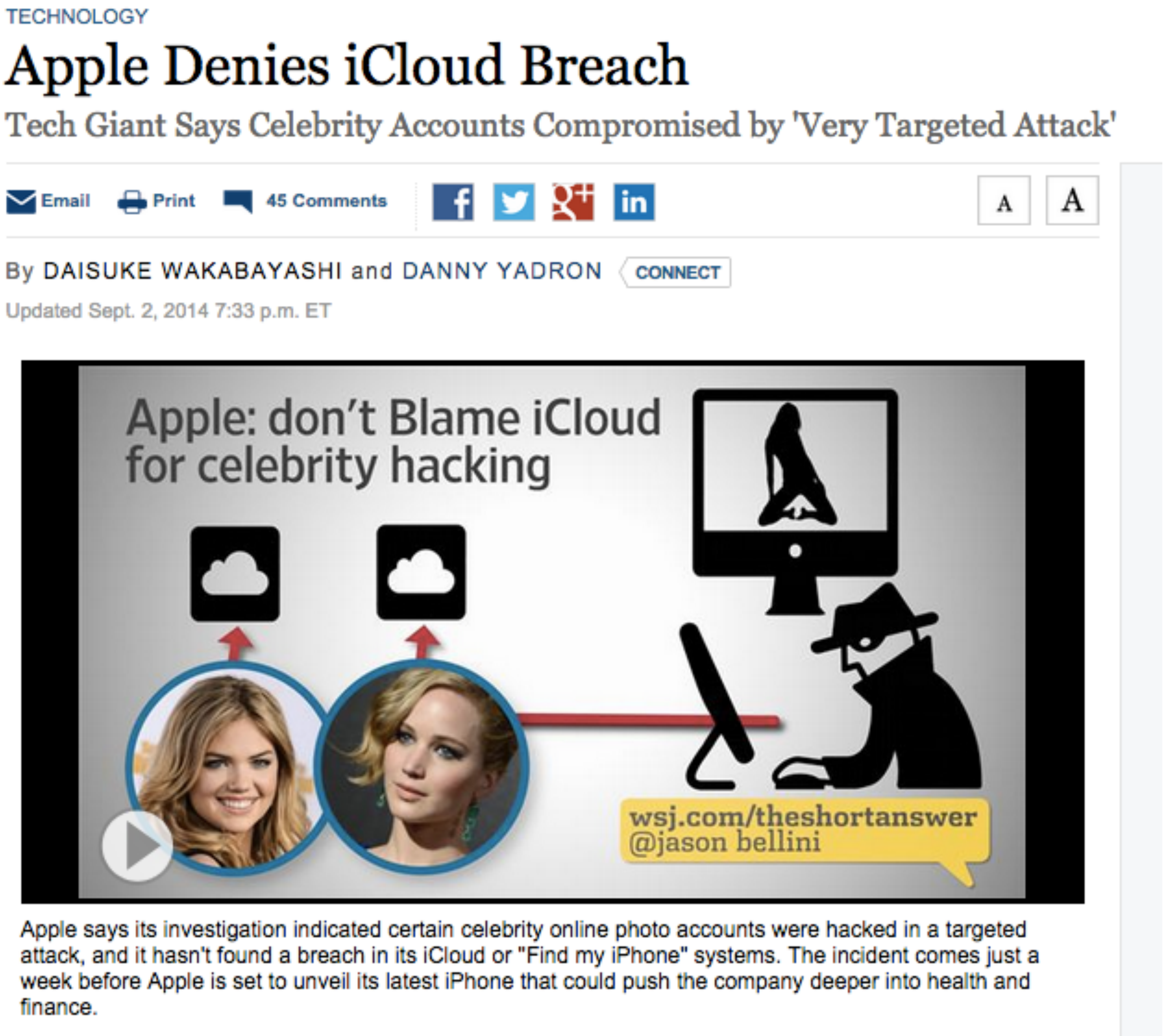
The result?

- Honan hadn’t backed up his data.
- He lost all of it, e.g., irreplaceable photos young daughter
- Why did hackers wipe his devices?
  - Just to prevent his regaining control of accounts!
- Honan’s suggested remedy… maybe in a later class…
- Honan got in touch with one of the hackers, Phobia, via instant messaging…

Quoth Phobia:

- “yea i really am a nice guy idk why i do some of the things i do.”
- “idk my goal is to get it out there to other people so eventually every1 can over come hackers”
- “even though i wasnt the one that did it i feel sorry about that. Thats alot of memories im only 19 but if my parents lost and the footage of me and pics i would be beyond sad and im sure they would be too.”

And yet, last year…



TECHNOLOGY

Apple Denies iCloud Breach

Tech Giant Says Celebrity Accounts Compromised by 'Very Targeted Attack'

By DAISUKE WAKABAYASHI and DANNY YADRON

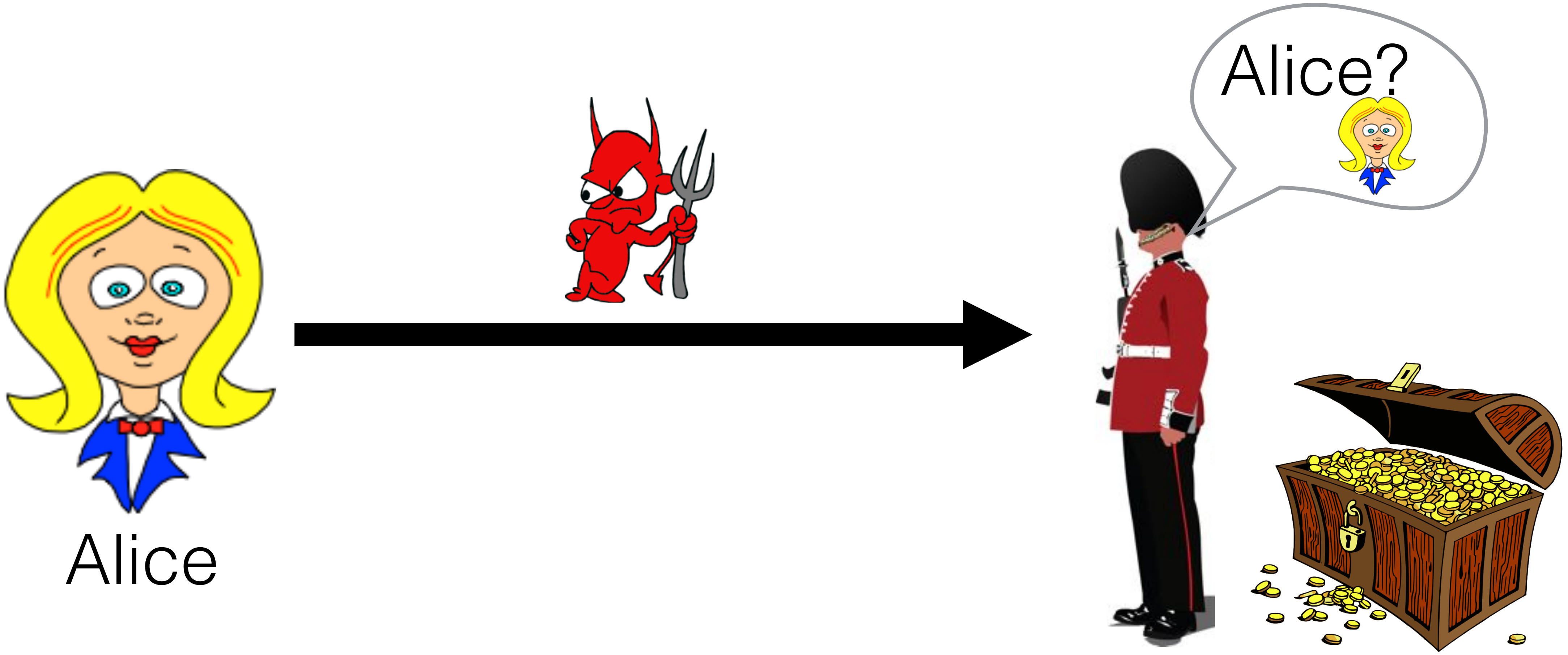
Updated Sept. 2, 2014 7:33 p.m. ET

Apple says its investigation indicated certain celebrity online photo accounts were hacked in a targeted attack, and it hasn't found a breach in its iCloud or "Find my iPhone" systems. The incident comes just a week before Apple is set to unveil its latest iPhone that could push the company deeper into health and finance.

User authentication

User authentication is proving your identity to a system (or another person).

- The starting point of nearly any security protocol.



The different mechanisms for user authentication

2015 Verizon Data Breach Investigations Report (DBIR): More than 50% of web app attacks were executed using stolen credentials

L

- Facebook “Trusted Contacts”
- Contextual authentication

How do people pick their passwords?

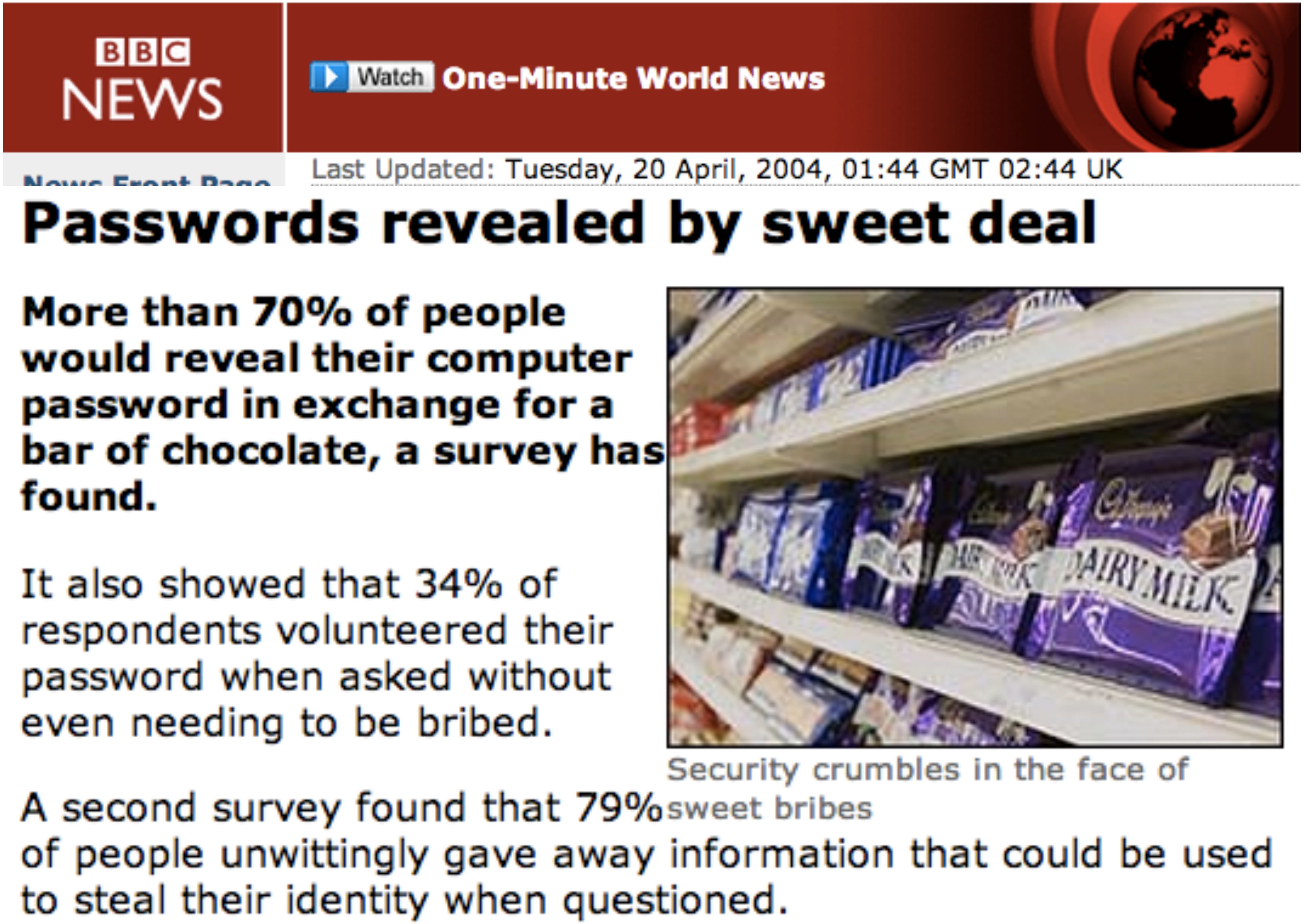
Often they don’t!

- In April 1994, English teenager (“Datastream Cowboy”) penetrated Pentagon computers via the Air Force Rome (New York) Laboratory, started probing Korean nuclear facilities.
  - Deemed “No. 1 threat to U.S. military”.
  - How did he do it?
    - Guessed default guest password!
- Surveys show that half of users leave the default password in place for their routers at home.
    - E.g., A. Tsow et al., “Warkitting: the Drive-by Subversion of Wireless Home Routers.” The Journal of Digital Forensic Practice, 2006
- Canary: cybersecurity@home

Often they don’t!

- Examples from Kevin Mitnick’s *Art of Intrusion*
- NY Times employee database: pwd = last 4 SSN digits
- “Dixie bank”: 99% of employees used password “password123”
- What’s the most important thing in the world to prevent unauthorized access to?
    - Nuclear missiles!
        - From 1962 to 1977, the passcode for launching Minuteman missiles was… 00000000.
        - Strategic Air Command was more afraid of lost passwords than of Armageddon!

How might a researcher collect passwords?



Last Updated: Tuesday, 20 April, 2004, 01:44 GMT 02:44 UK

Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.

A second survey found that 79% of people unwittingly gave away information that could be used to steal their identity when questioned.

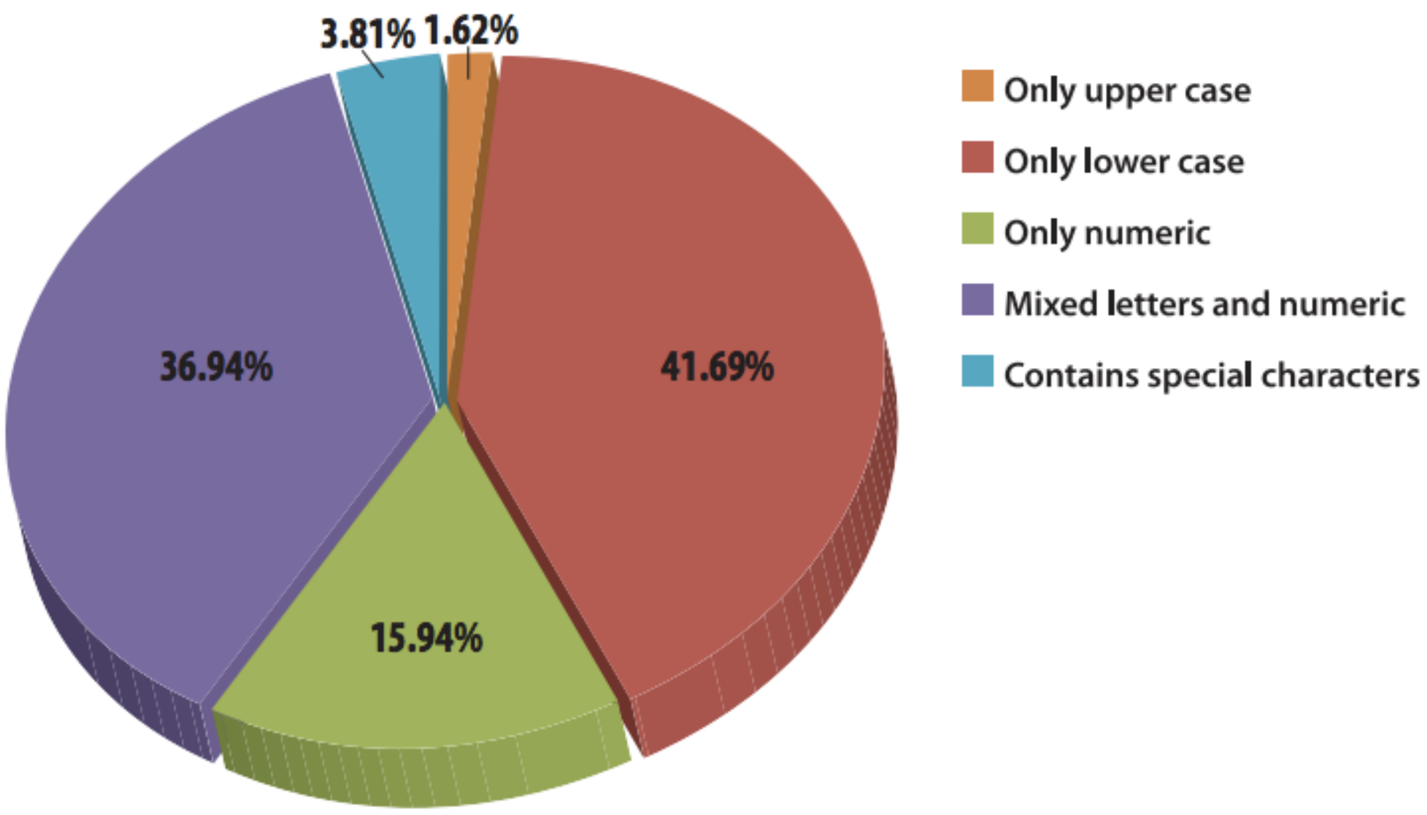
Security crumbles in the face of sweet bribes

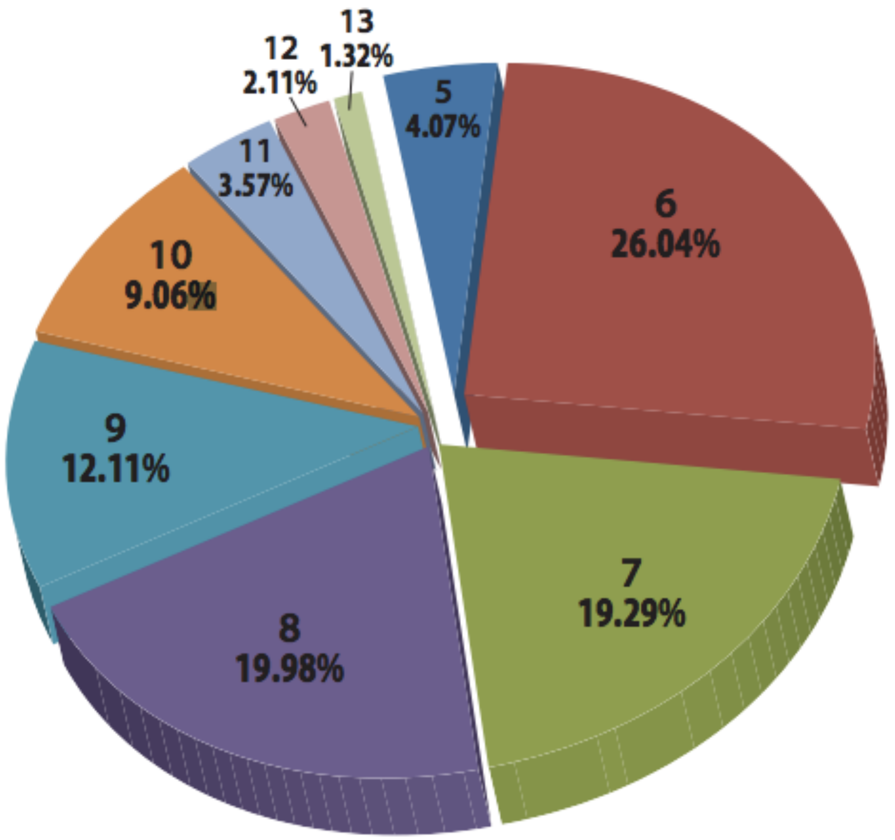
Another way

rockyou

- “Social gaming” site RockYou hacked in December 2009
  - SQL injection attack; good example of how breaches occur— more in a later lecture
- Disclosed 32 million user passwords; posted to internet
- Passwords were in clear (not hashed or encrypted)
- Main source today of research / knowledge about user password composition

Some findings

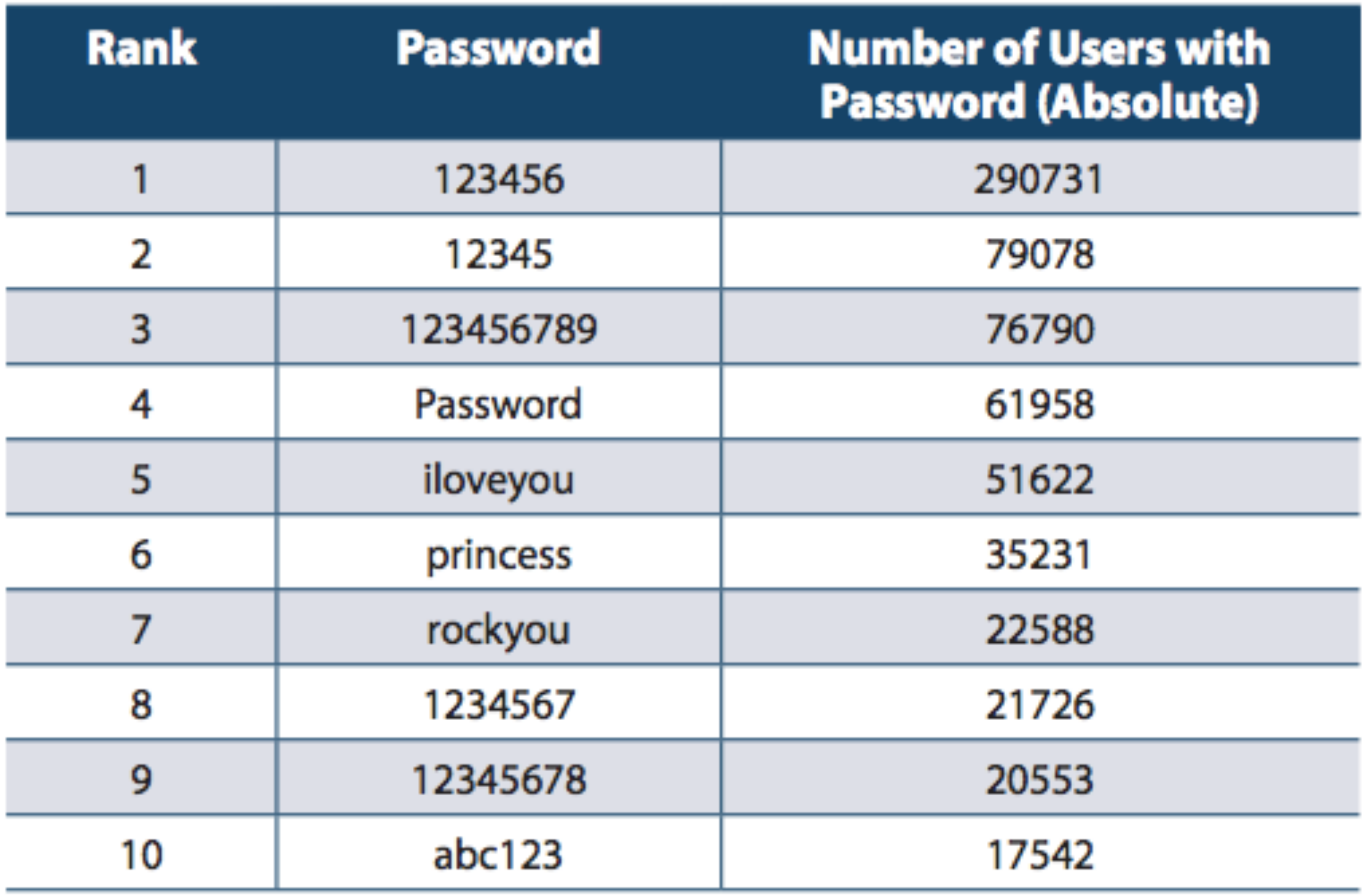




Password Length Distribution

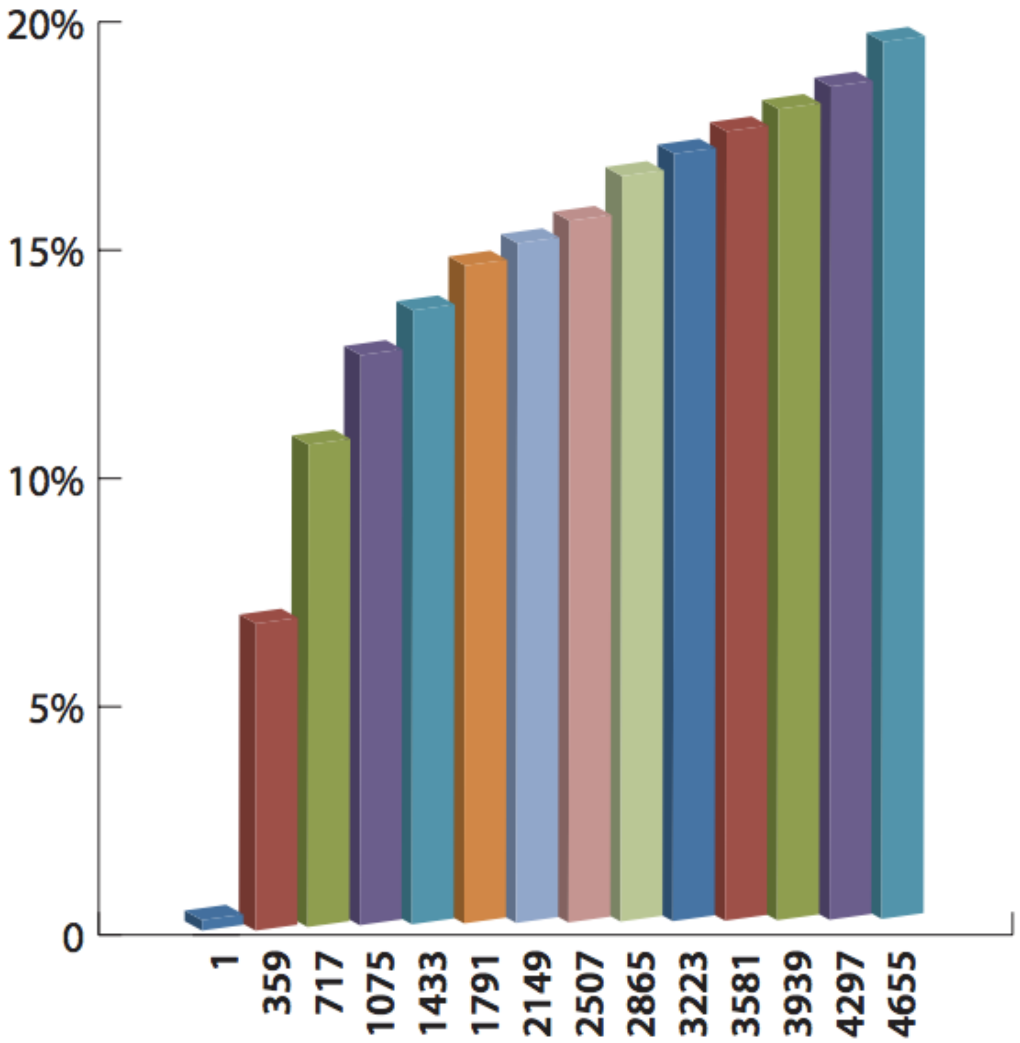
Source: Imperva. Consumer Password Worst Practices. 2014.

Worth even a candy bar?



Rank	Password	Number of Users with Password (Absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Top 10 RockYou passwords

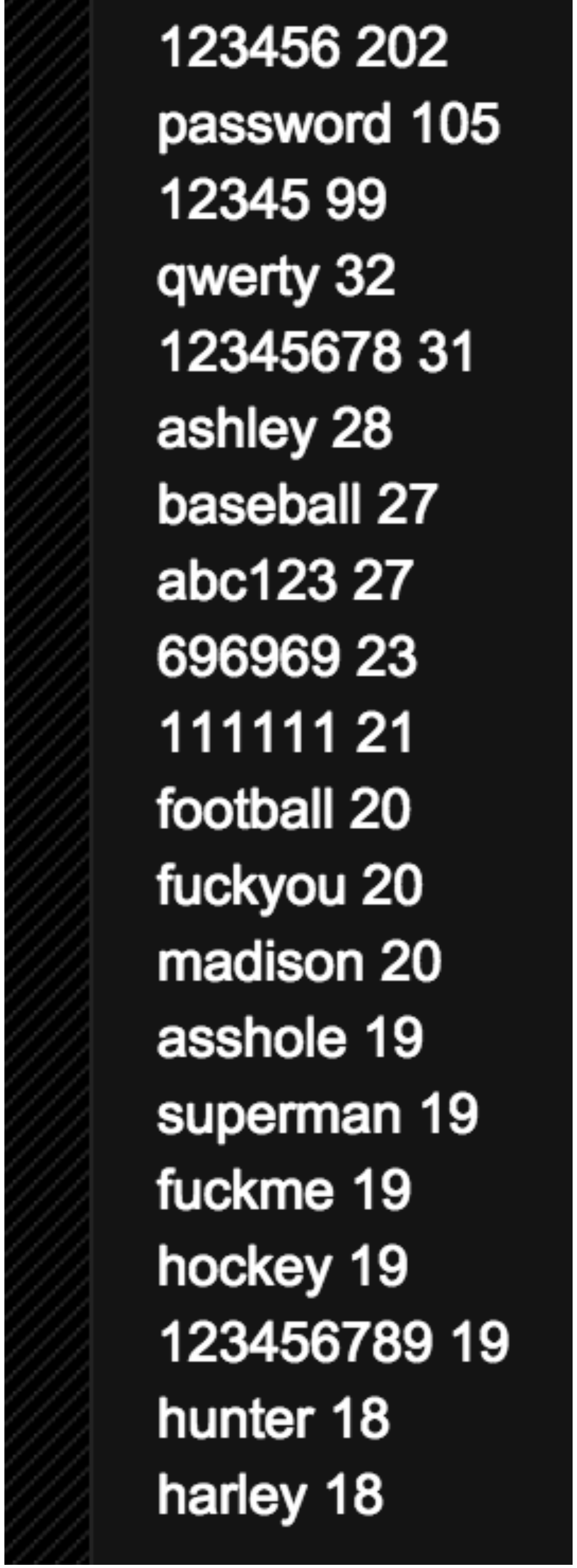


Accumulated Percent of Dictionary Attack Success

Source: Imperva. Consumer Password Worst Practices. 2014.

From Ashley Madison breach

- Result of cracking 4007 passwords
  - Top 20 worst passwords…
- Very similar to RockYou
  - Just a rather less polite…
  - And no 'iloveyou'



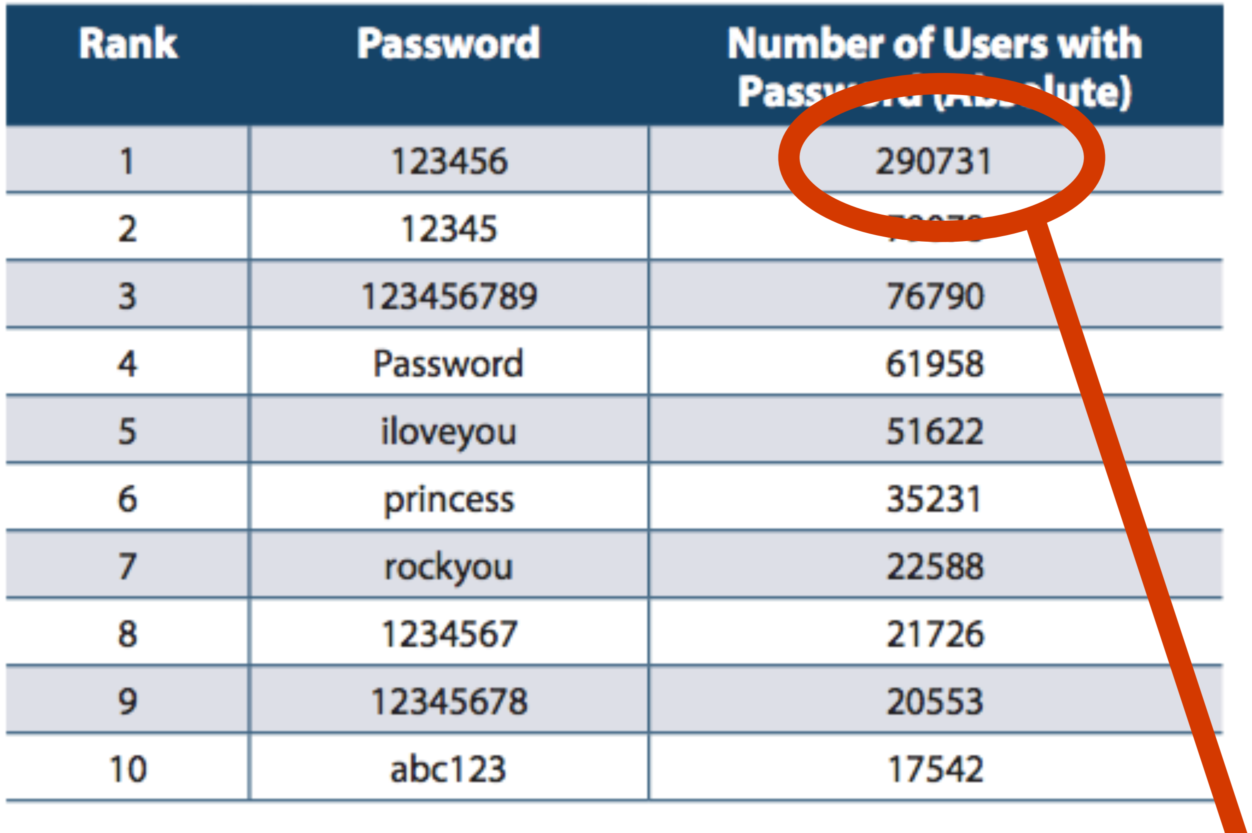
123456	202
password	105
12345	99
qwerty	32
12345678	31
ashley	28
baseball	27
abc123	27
696969	23
111111	21
football	20
fuckyou	20
madison	20
asshole	19
superman	19
fuckme	19
hockey	19
123456789	19
hunter	18
harley	18

Source: http://www.pxdojo.net/2015/08/what-i-learned-from-cracking-4000.html

Measuring password strength

- Many ways to measure password strength
- “Entropy”: intuitively, the “randomness” of passwords over a population, and thus how hard for attacker to guess
- One important type:
    - *Min-entropy:* related to commonness of most popular password
- We’ll let “guessing probability” or GP denote probability of most probable password over a population; and GPP denote the (unique) password with the GP
    - Formally, for random variable Y with probability distribution $P_Y(y)$, min-entropy (in bits) is $H_{\min}(Y) = -\log_2 \max_{y \in Y}(P_Y(y))$. Max probability is 2^{-$H_{\min}(Y)$}.

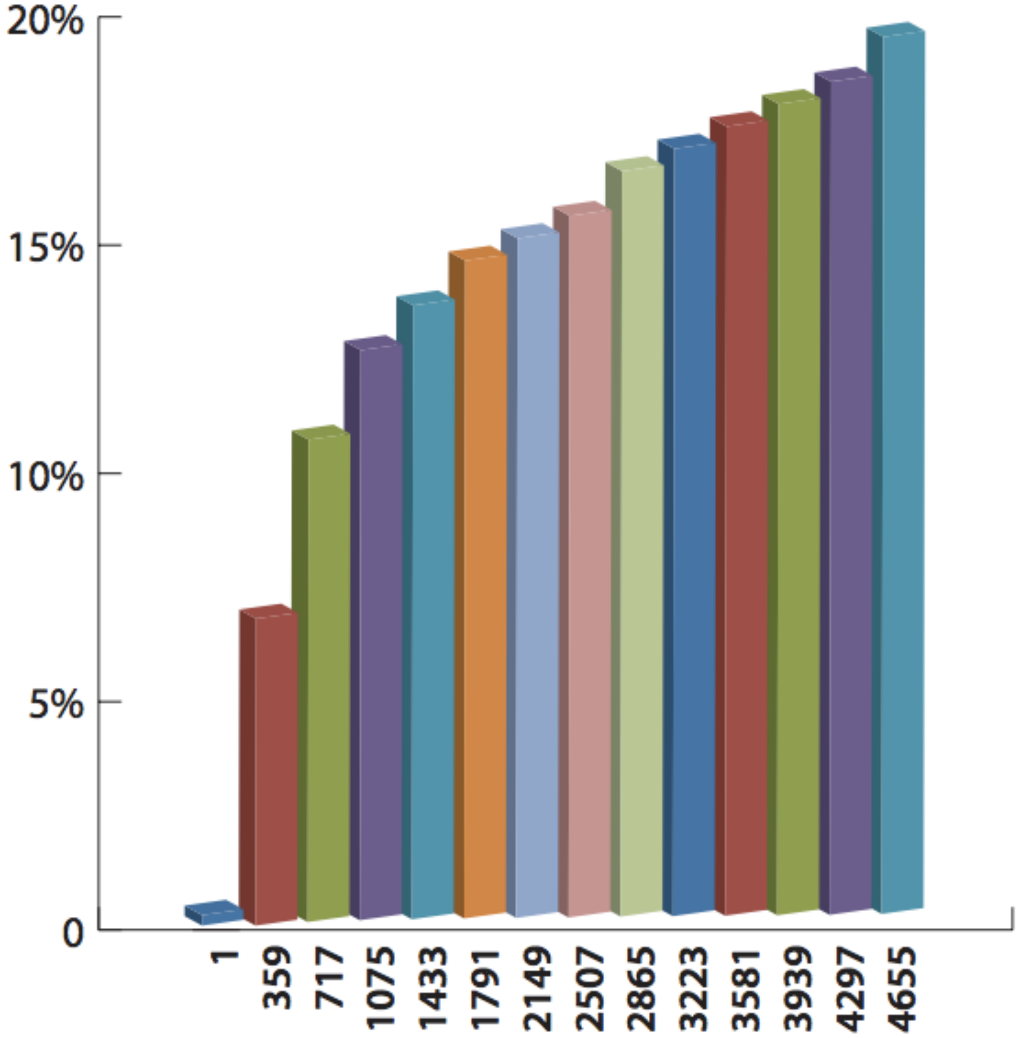
Guessing probability



Rank	Password	Number of Users with Password (Absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Top 10 RockYou passwords

GP = 0.9%; i.e., 0.9% of users, about 1 in 111, have this password!



Accumulated Percent of Dictionary Attack Success

- In 2013 Adobe breach, GP = 1.6%, and GPP was "123456"!

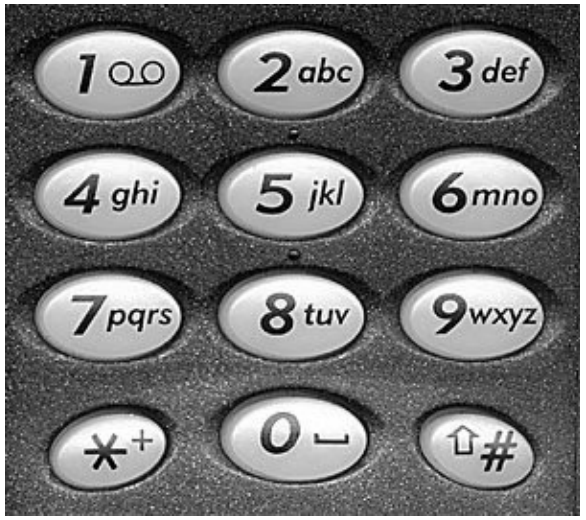
Source: Imperva. Consumer Password Worst Practices. 2014.

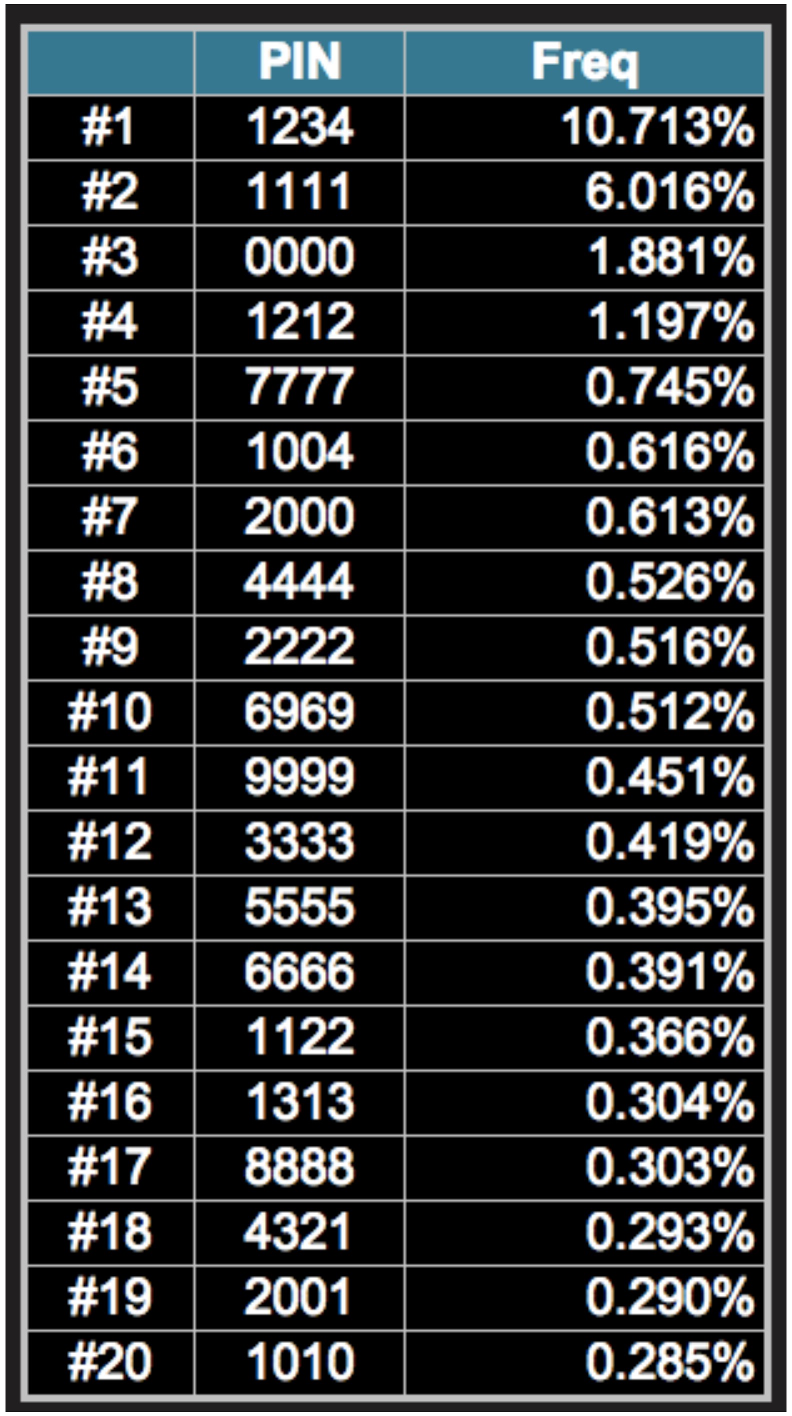
Why is GP important?

- Measures vulnerability of the weakest accounts, which can be best for an attacker to target.
- If you get only a single guess at a password, you should guess the GPP.
  - Prob. of success is GP (about 0.9% for RockYou).
- If you can attack multiple accounts, best strategy is to try GPP against them sequentially.
  - Success in an expected (average)1 / GP tries (about 111 for RockYou!)

People also choose poor PINs

- GP for PINs is 10%+!
  - I.e. you have a 1/10 chance of guessing a random person’s PIN correctly!
- GPP is…
  - 1234 (of course!)
- Another popular PIN:
  - 2580 (Why?)



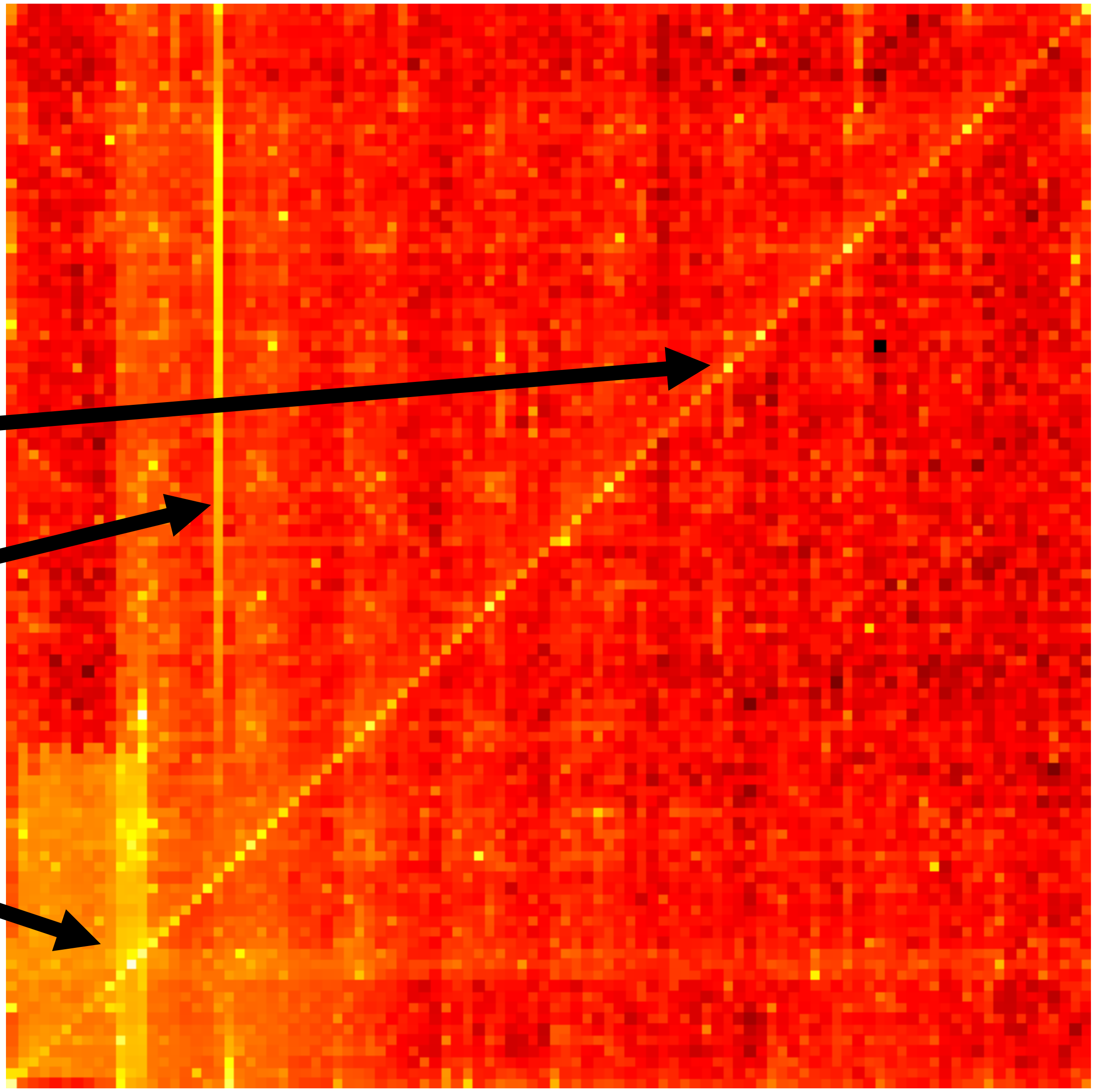


	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Source: N. Berry. Datagenetics. 3 Sept. 2012.

A PIN heatmap

Other interesting insights into how people think about PINs…



Repeated couplets (e.g., 0101) on diagonal

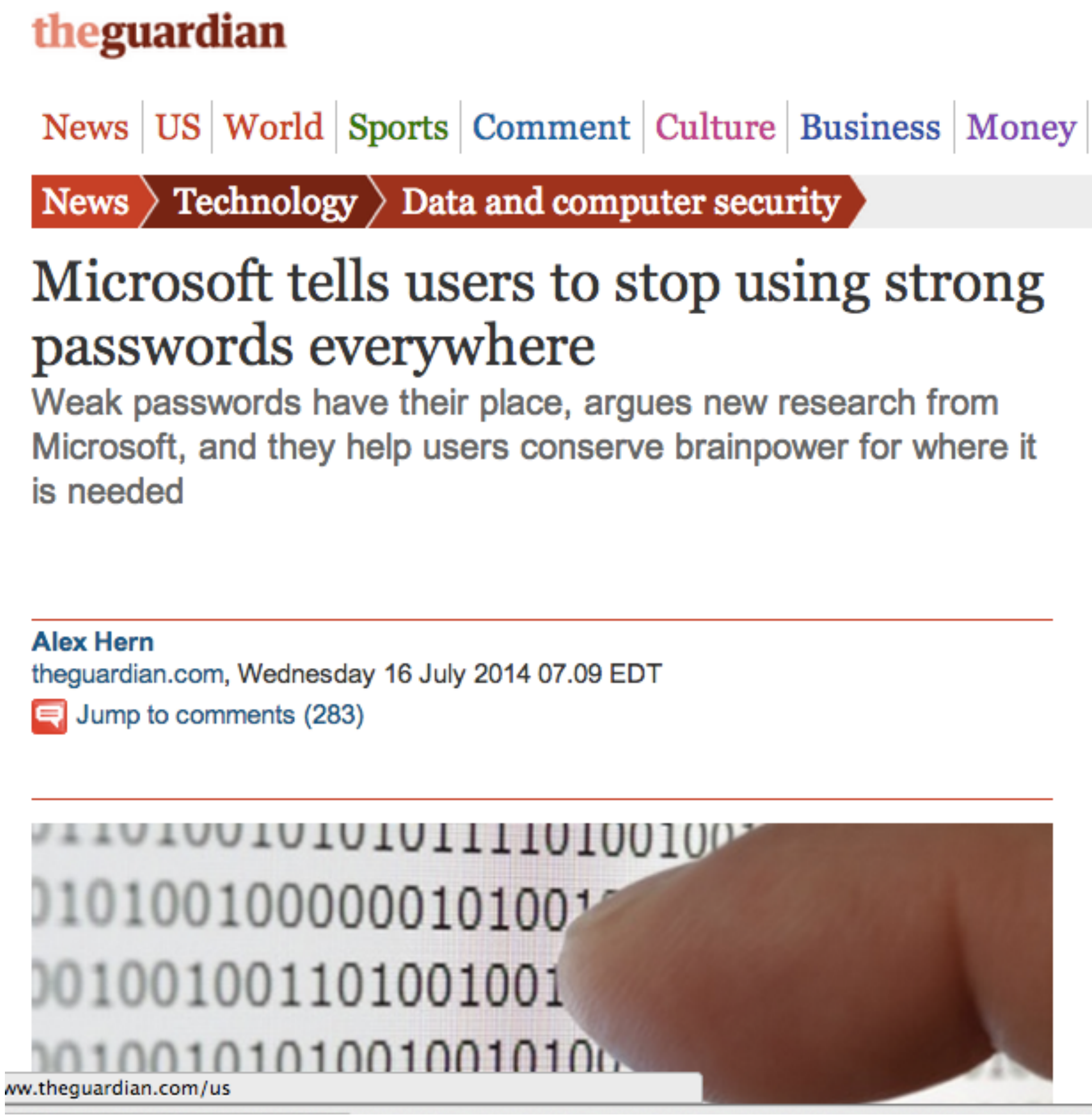
Years 19YY are here

DDMM dates are in this mass

Source: N. Berry. Datagenetics. 3 Sept. 2012.

But maybe users aren’t stupid after all…

- A recent paper…
  - D. Florencio, C. Herley, and P. van Oorschot. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. USENIX Security, 2014.
- Recall **incentives**.
- Remembering passwords imposes *cognitive load*
  - Burden on memory
- To optimize security *and* cognitive load, Florencio et al. observe need for weak passwords in portfolio


theguardian
News | US | World | Sports | Comment | Culture | Business | Money
News › Technology › Data and computer security
ww.theguardian.com/us

Microsoft tells users to stop using strong passwords everywhere

Weak passwords have their place, argues new research from Microsoft, and they help users conserve brainpower for where it is needed

Alex Hern
theguardian.com, Wednesday 16 July 2014 07.09 EDT
Jump to comments (283)

How are passwords protected on servers?

And why are strong ones important?

Not all that well…
some losses…

Adobe

130 million (ECB-encrypted) passwords
Oct. 2013

YAHOO

273 million passwords
2014

livingsocial

50 million passwords
April 2014

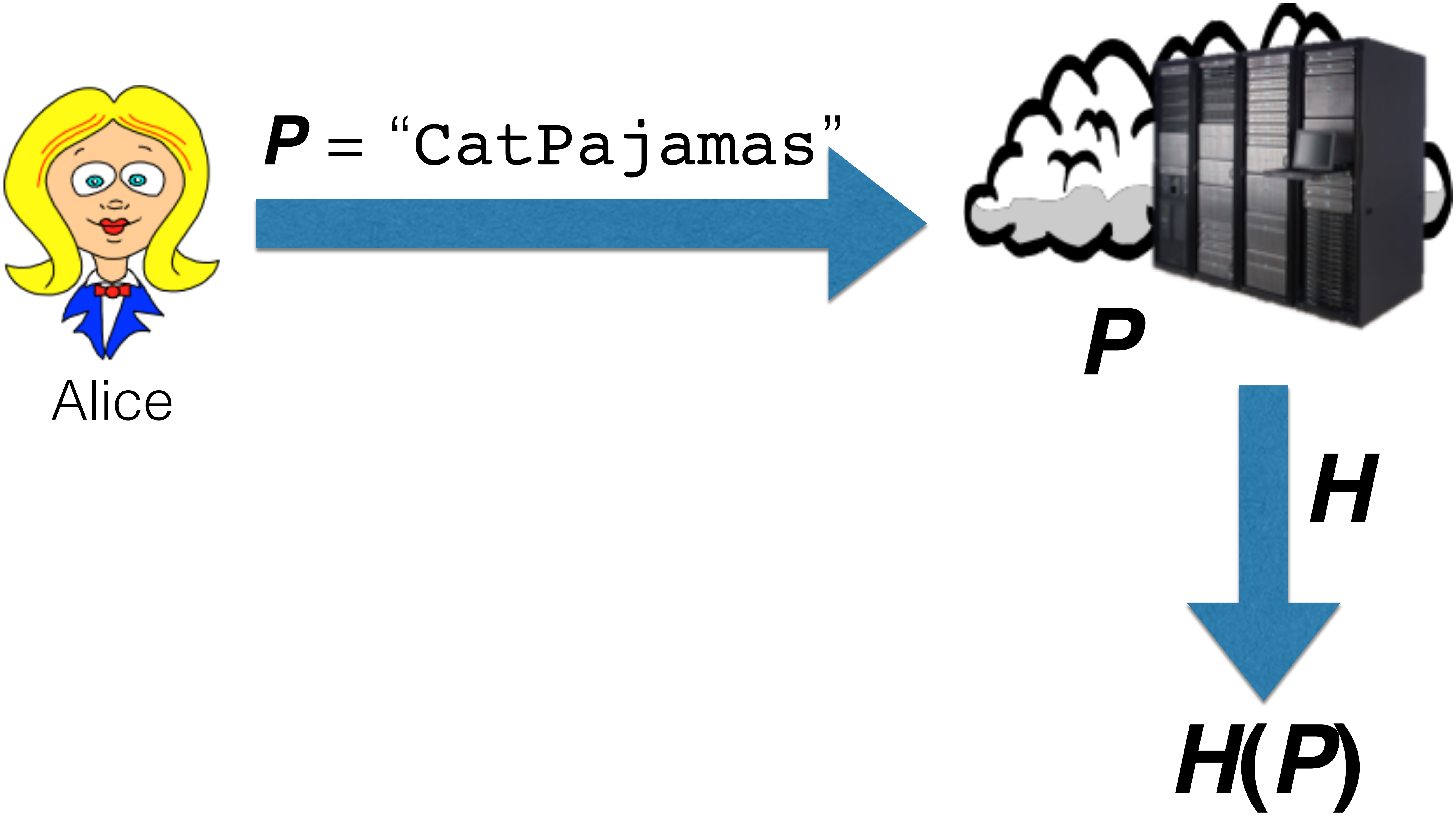
36 million passwords
August 2015

EVERNOTE

50 million passwords
March 2013

Plus LivingSocial, Last.fm, eHarmony, etc. etc. etc.

Passwords are generally protected via hashing



Alice

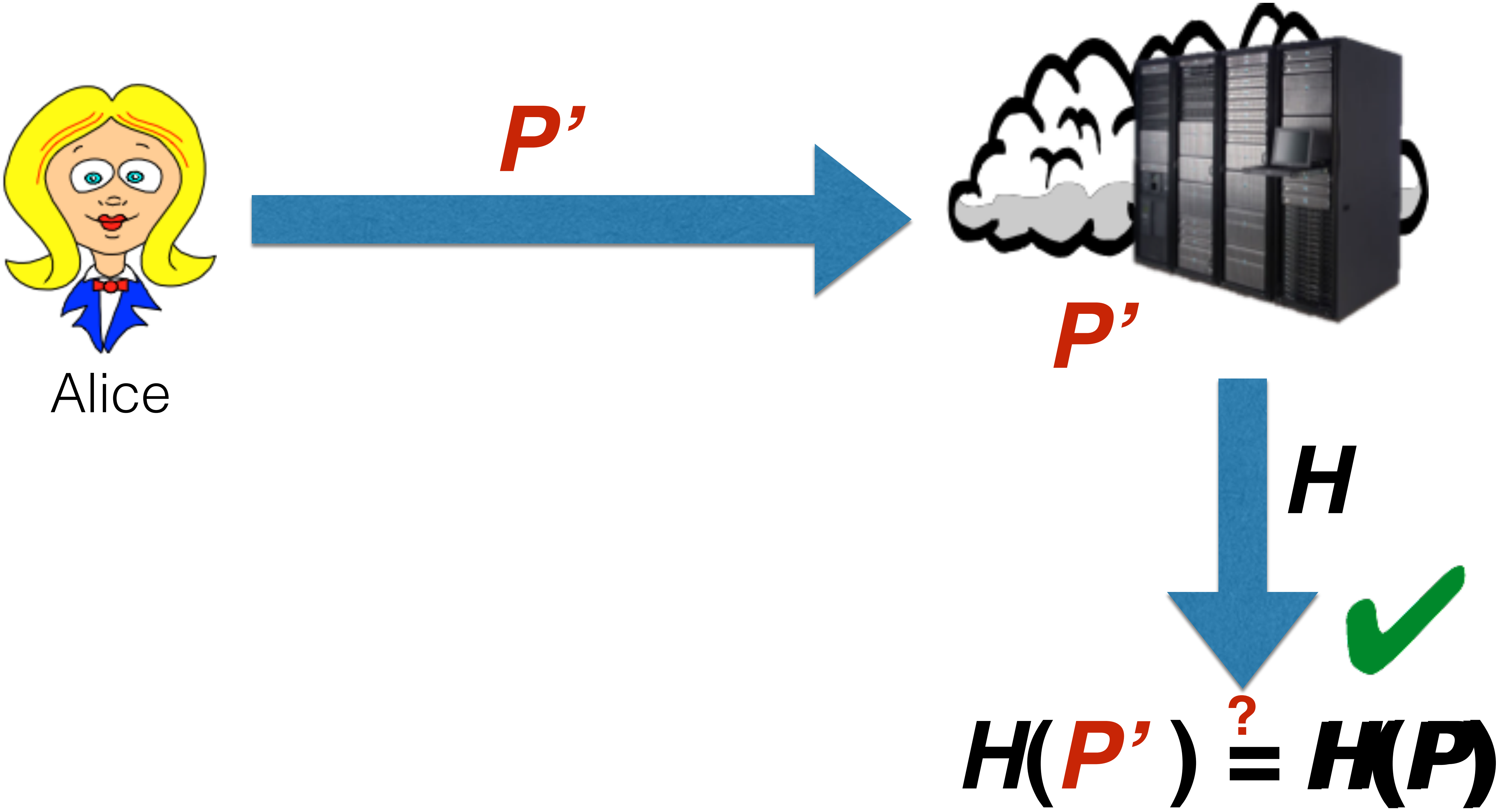
P = "`CatPajamas`"

P

H

***H*(*P*)**

To verify an incoming password…



$H(P') \overset{?}{=} H(P)$

Hashing

- A hash function *H*(*P*) applied to password *P* has a one-wayness property:
  - It is possible to *verify* whether *P'* is the correct password, i.e., *P'* = *P.*
    - Compute *H(P')* and see if *H(P')* = *H(P)*
  - Otherwise, nothing can be learned about *P* from *H*(*P*).
- This seems great. If the system gets breached and hashes are leaked, passwords aren't leaked.
- At least, not directly…

Hashing

- Unfortunately, the ability to check *P’* leaks a lot of information…
- An attacker that learns *H*(*P*) can keep testing guesses *P’* until she guesses *P* itself.
- This kind of brute-force guessing is known as *password cracking*.

The art of password cracking

- Password crackers are software that performs brute-force guessing attacks against password hashes
- Basic password crackers guess common passwords, trying:
  - Dictionary words
  - Dictionary words spelled backwards
  - Proper names—people, streets, cities
  - License plate numbers
  - Plus various manipulations:
    - Upper case / lower case
    - LEET substitutions
      - E.g., a <- @, etc.

If you've thought of it, they can too…

The art of password cracking

The tools just keep getting better:

- John the Ripper
  - Developed originally for Unix hash; now available for many hash types
  - GUIs such as Johnny bring tool within reach of nonspecialists
- Weir et al. (2009) cracker
  - Uses probabilistic context free grammars to model user password selection in the wild
  - 28% to 129% faster than John the Ripper
- RockYou was a boon for cracking!

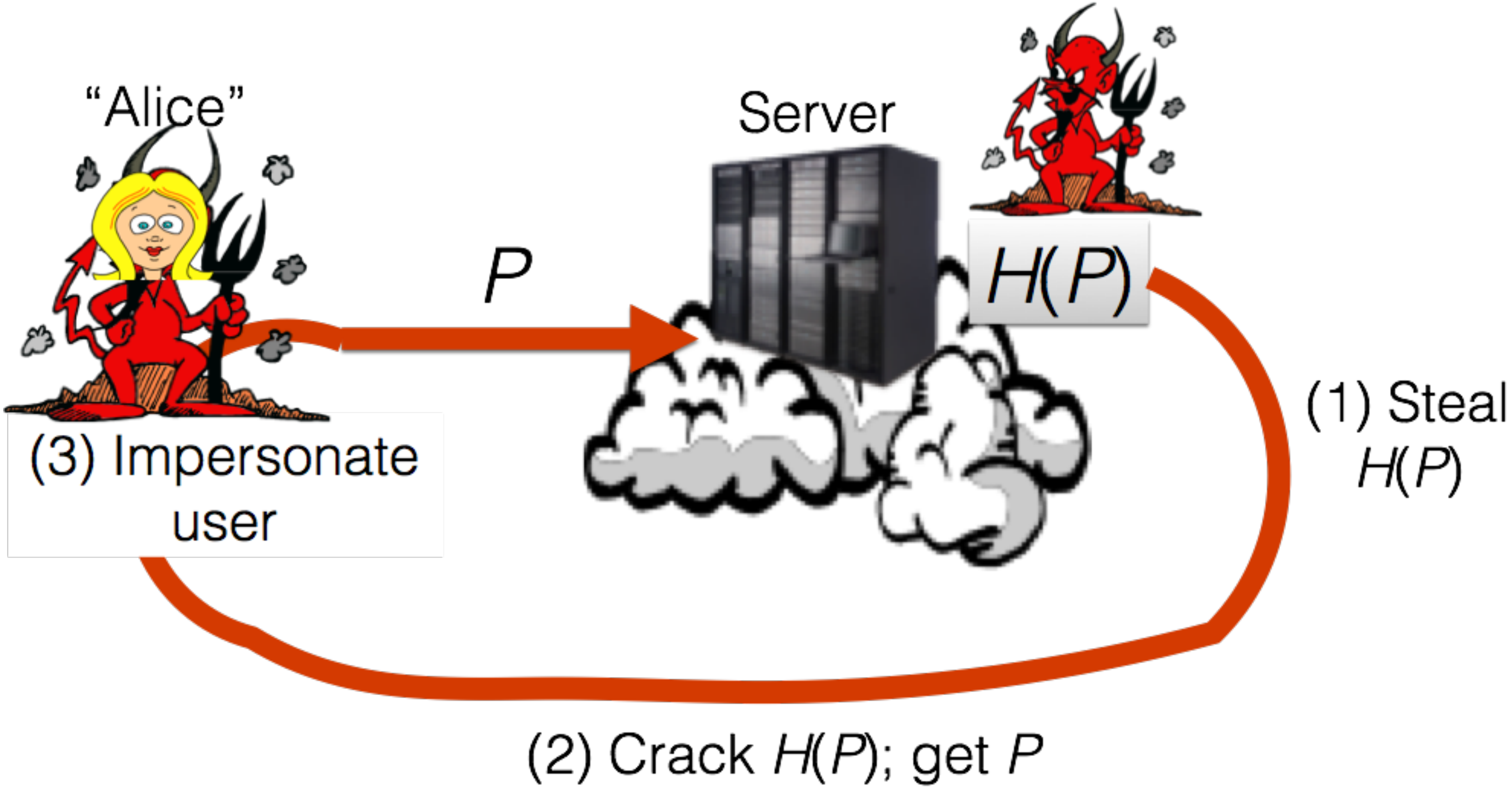
…and they're getting faster

- Custom GPU-based hardware
  - A 5-server rig with 25 Radeon GPUs
  - 77 million md5crypt-hashed passwords per second
    - md5crypt() is used by FreeBSD and Linux
- Cloud-based cracking tools
  - CloudCracker, Cloud Cracking Suite (CCS)
  - Can use cloud-based browsers to do MapReduce jobs (almost) for free
    - Tenduklar et al. Abusing Cloud-Based Browsers for Fun and Profit. ACSAC, 2012.

Slide source: V. Shmatikov, 2014

Source: https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/

Password attack path



“Alice”

Server

P

$H(P)$

(1) Steal $H(P)$

(2) Crack $H(P)$; get P

(3) Impersonate user

Given password risks, why can’t users follow short, sweet, sensible advice like this?

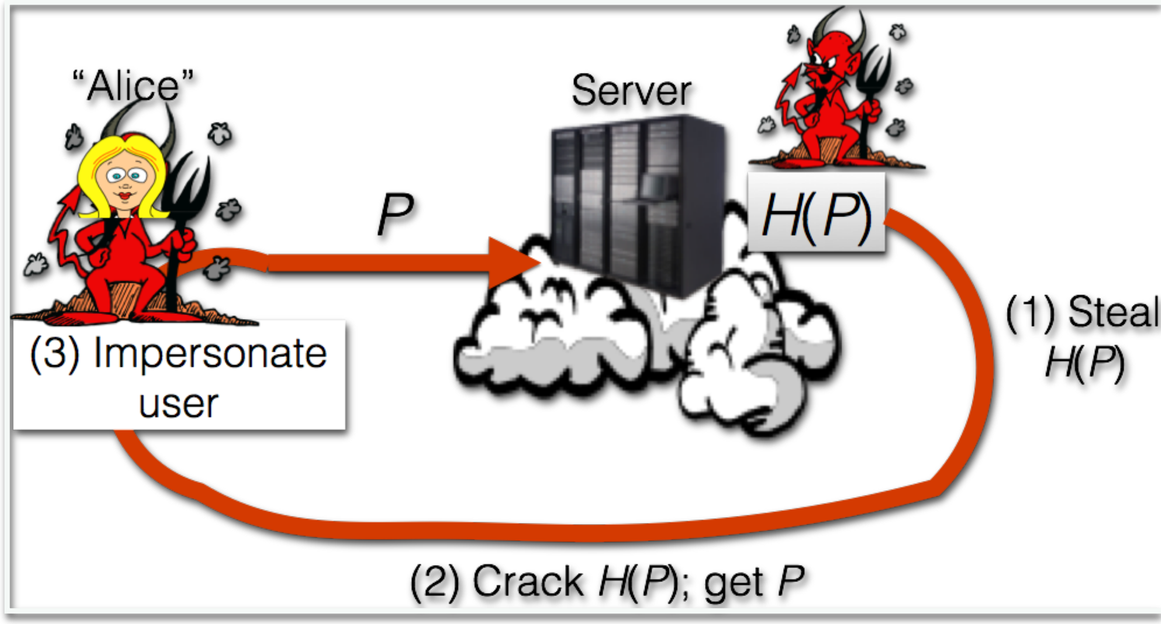
David Curry. Improving the Security of Your UNIX System. SRI International, 1990. (Still cited today)

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.
- Do use a password with mixed-case alphabetics.
- Do use a password with nonalphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so **you don't have to write it down.** [My emphasis]
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Times have changed

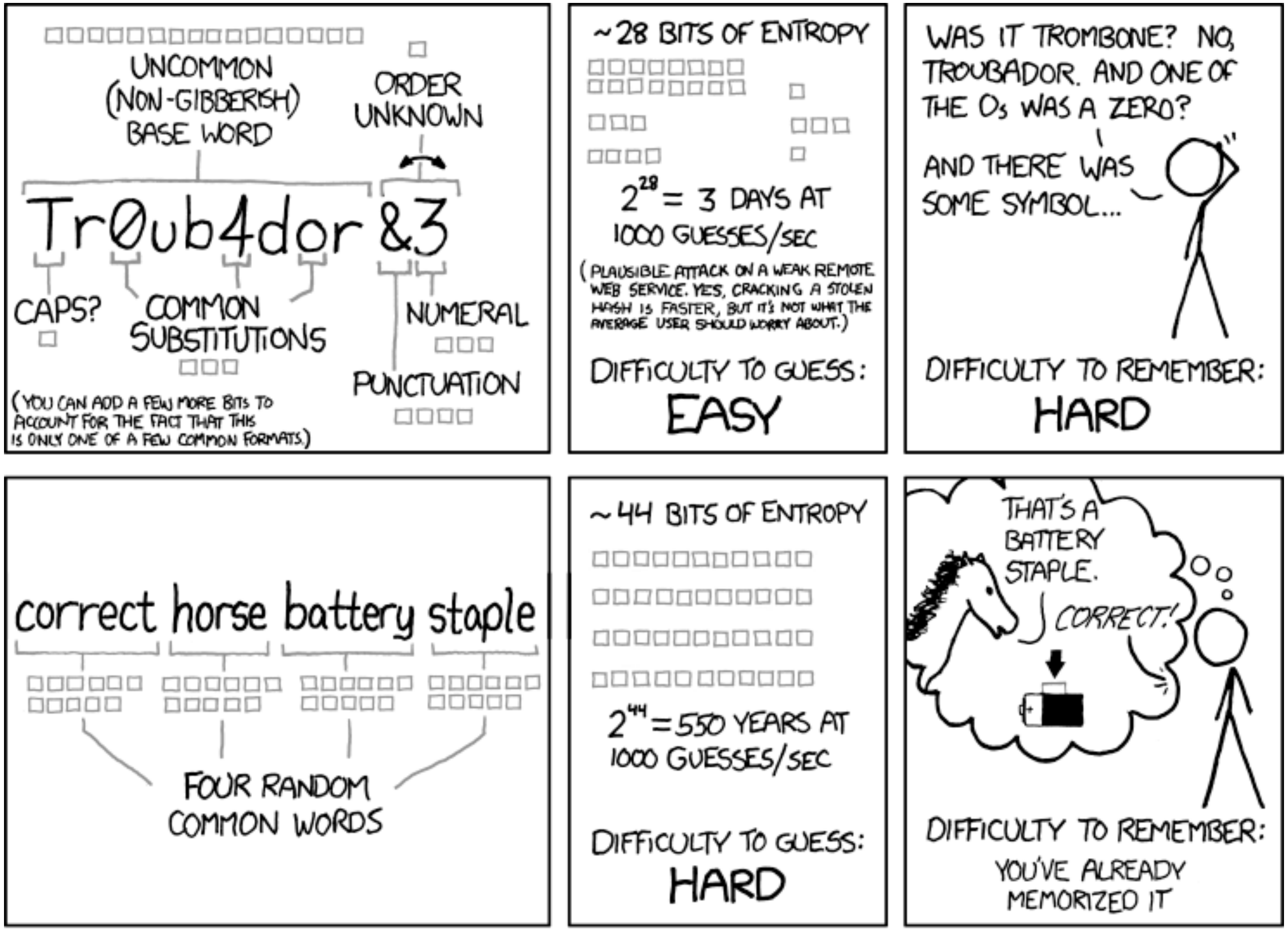
- Note missing advice:
  - `Don't use the same password on multiple websites.`
- Average user has many passwords now
  - At least 25 per user (probably higher today) [Florencio & Herley, 2007]

Some key points



- Strong passwords serve two goals.
  - They prevent online guessing attacks.
  - They prevent offline cracking attacks.
- Mainly useful for the latter. Why?
  - Online guessing can be throttled, i.e., slowed / stopped by service provider
  - Offline guessing can be performed arbitrary number of times
- Users are being required to protect themselves in case password hashes leak when systems get breached.
- *The industry is basically forcing users to protect themselves against its mistakes!*

Password advice comes from… xkcd


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.

Other common ways passwords get compromised

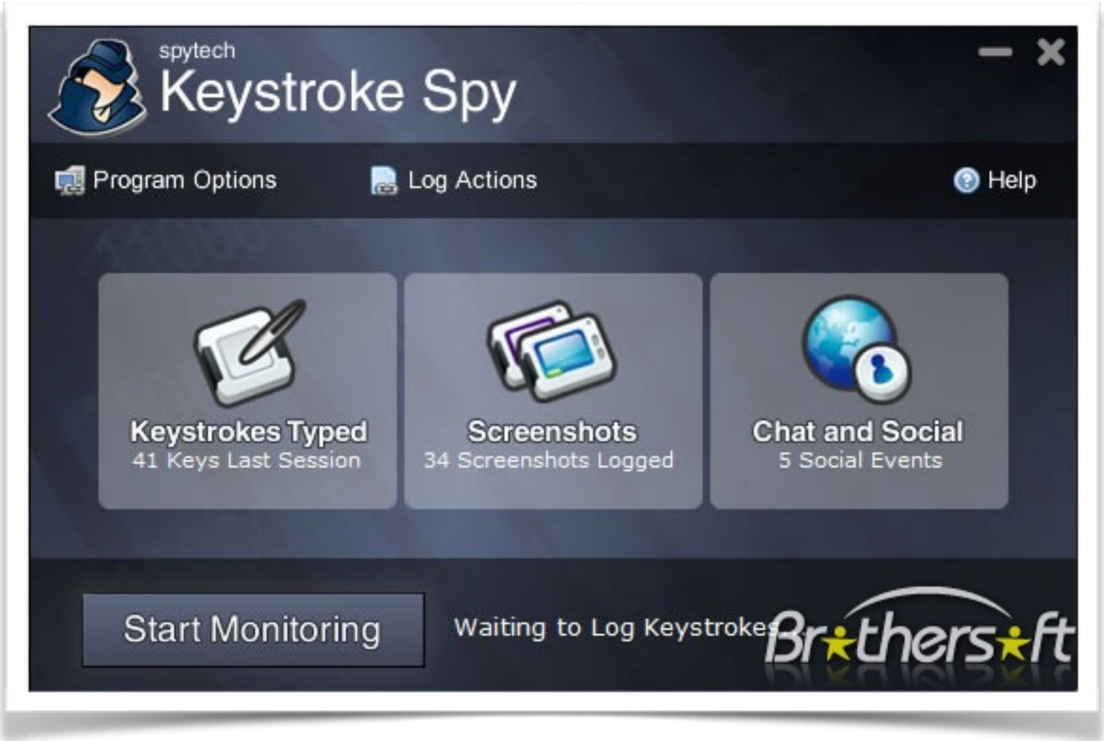
- Social engineering
  - 2007 study by Treasury Dept. found that 61 of 102 employees could be convinced by “IT help desk” to change passwords.
- Password reuse across sites
  - Users average about 6 sites per password! (Florencio and Herley (2007))

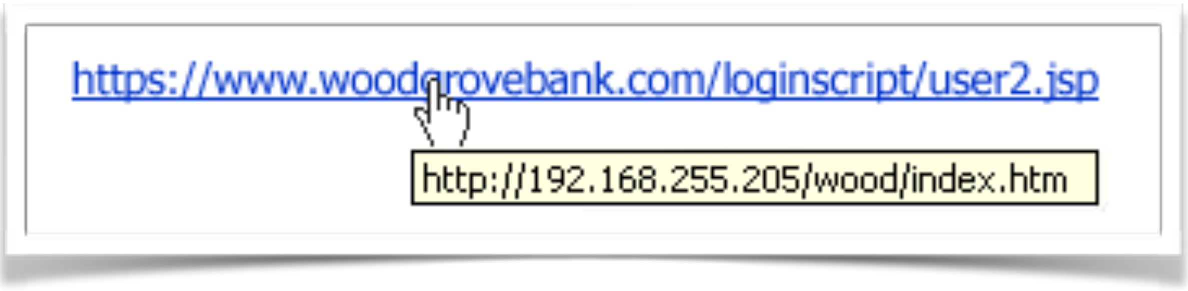
Other common ways passwords get compromised

- Default passwords
- Illustrated by Gary McKinnon
  - Self-labeled “bumbling computer nerd”
  - In 2001 and 2002, hacked into 97 US military and NASA computers searching for evidence of free energy suppression and UFO coverups
    - “… shut down the entire US Army’s Military District of Washington network of over 2000 computers for 24 hrs”
    - “… rendered [US Naval Weapons Station Earle]’s entire network of over 300 computers inoperable at a critical time immediately following 11 September 2001”
  - Method: Perl script randomly looking for blank and default passwords to administrator accounts

Other common ways passwords get compromised

- Malware
- Phishing
  - $1.5 billion lost to phishing in 2012 (RSA Feb. 2013 Fraud Report)
  - Can be highly sophisticated, as we'll discuss in a lecture on social engineering…
  - How did RSA get breached in 2010?




https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

…and some exotic ones

E.g., reflections

- Raguram et al. iSpy: automatic reconstruction of typed input from compromising reflections. ACM CCS, 2011.

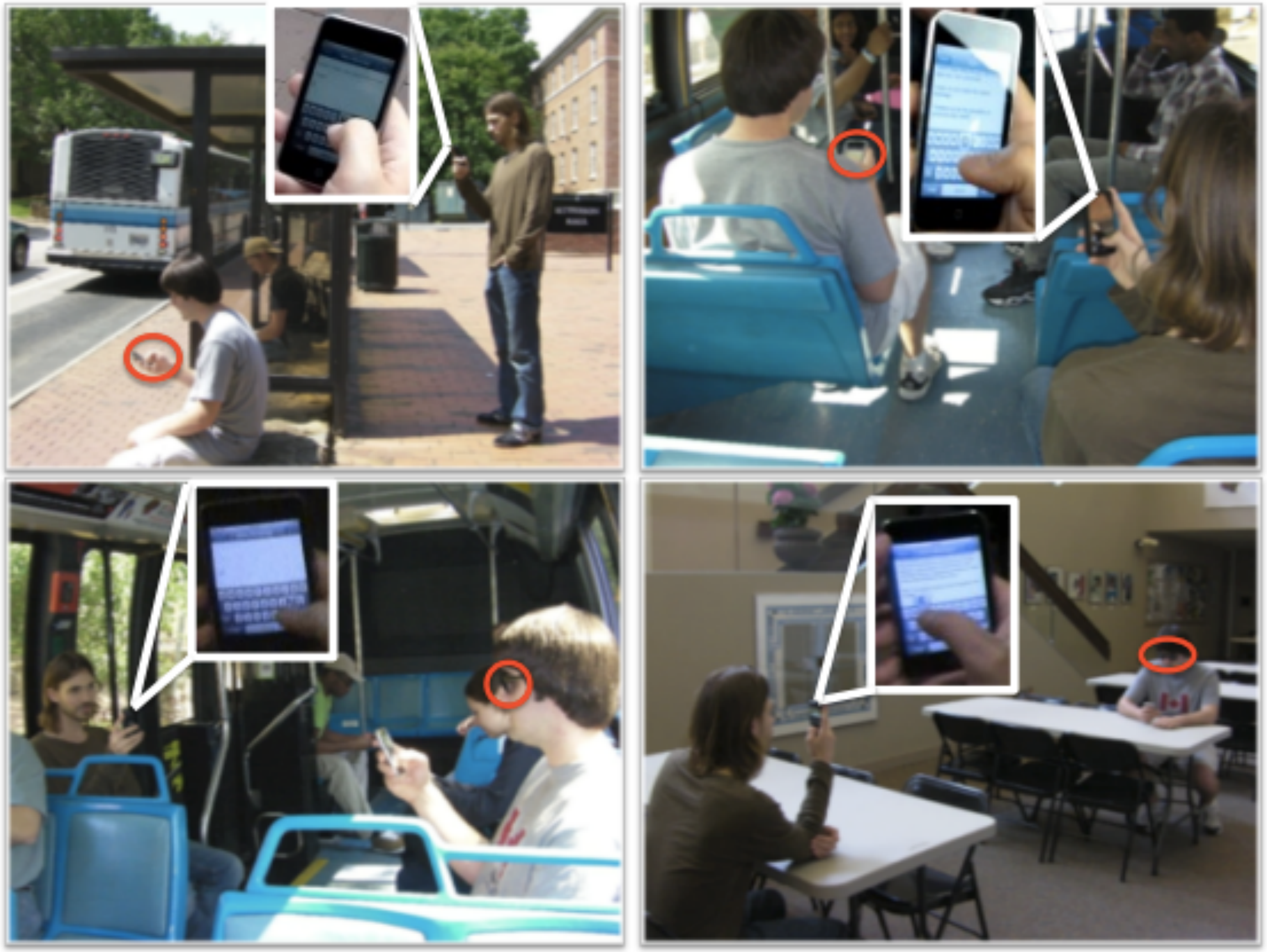
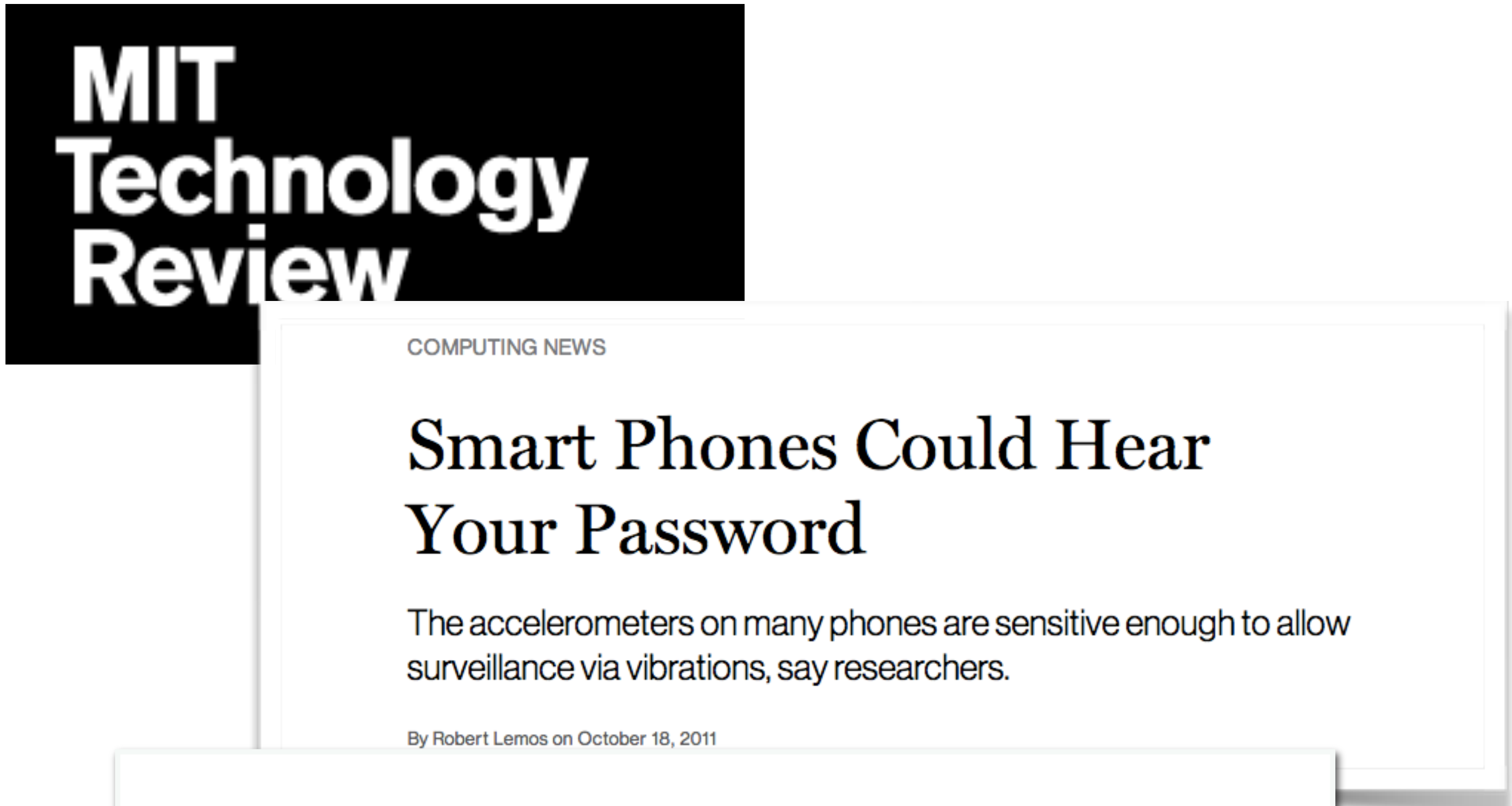


Figure 1: Some example threat scenarios that we investigated. Video was recorded in both indoor and outdoor environments, using various consumer video cameras. top: shoulder surfing, bottom: reflection surfing, bottom right: key *pop-out* event.

…and some exotic ones

Vibrations

- Philip Marquardt et al. iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. ACM CCS, 2011.



MIT Technology Review

COMPUTING NEWS

Smart Phones Could Hear Your Password

The accelerometers on many phones are sensitive enough to allow surveillance via vibrations, say researchers.

By Robert Lemos on October 18, 2011

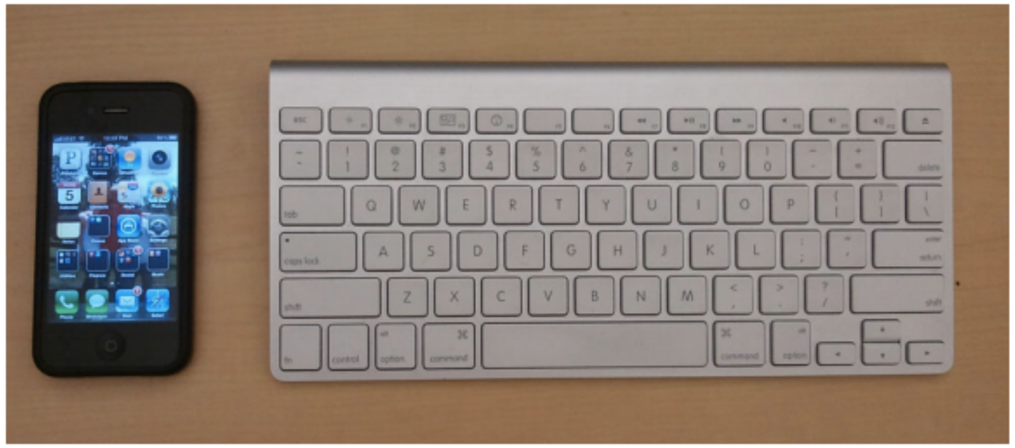
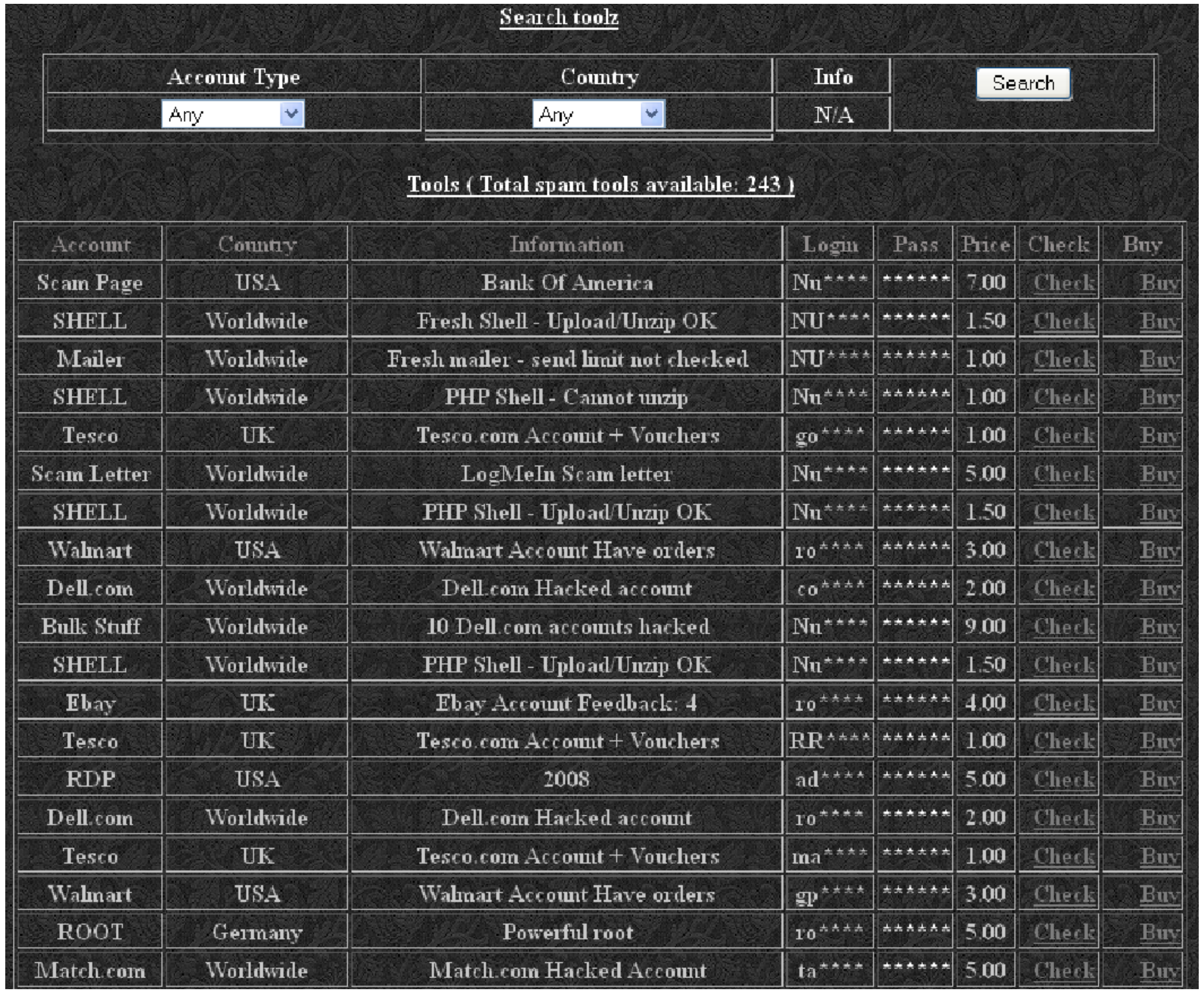


Figure 1: Our experimental placement of a mobile phone running a malicious application attempting to recover text entered using the nearby keyboard.

And there’s a vast market for stolen passwords

- Online retailer account passwords can go for $1-$5.
- Social media account passwords can now be worth more than stolen credit card numbers.
- Reports of $325+ prices for Twitter usernames / passwords.
    - Why?



Search toolz

Account Type	Country	Info	Search
Any	Any	N/A	

Tools (Total spam tools available: 243)

Account	Country	Information	Login	Pass	Price	Check	Buy
Scam Page	USA	Bank Of America	Nu****	******	7.00	Check	Buy
SHELL	Worldwide	Fresh Shell - Upload/Unzip OK	NU****	******	1.50	Check	Buy
Mailer	Worldwide	Fresh mailer - send limit not checked	NU****	******	1.00	Check	Buy
SHELL	Worldwide	PHP Shell - Cannot unzip	Nu****	******	1.00	Check	Buy
Tesco	UK	Tesco.com Account + Vouchers	go****	******	1.00	Check	Buy
Scam Letter	Worldwide	LogMeIn Scam letter	Nu****	******	5.00	Check	Buy
SHELL	Worldwide	PHP Shell - Upload/Unzip OK	Nu****	******	1.50	Check	Buy
Walmart	USA	Walmart Account Have orders	ro****	******	3.00	Check	Buy
Dell.com	Worldwide	Dell.com Hacked account	co****	******	2.00	Check	Buy
Bulk Stuff	Worldwide	10 Dell.com accounts hacked	Nu****	******	9.00	Check	Buy
SHELL	Worldwide	PHP Shell - Upload/Unzip OK	Nu****	******	1.50	Check	Buy
Ebay	UK	Ebay Account Feedback: 4	ro****	******	4.00	Check	Buy
Tesco	UK	Tesco.com Account + Vouchers	RR****	******	1.00	Check	Buy
RDP	USA	2008	ad****	******	5.00	Check	Buy
Dell.com	Worldwide	Dell.com Hacked account	ro****	******	2.00	Check	Buy
Tesco	UK	Tesco.com Account + Vouchers	ma****	******	1.00	Check	Buy
Walmart	USA	Walmart Account Have orders	gp****	******	3.00	Check	Buy
ROOT	Germany	Powerful root	ro****	******	5.00	Check	Buy
Match.com	Worldwide	Match.com Hacked Account	ta****	******	5.00	Check	Buy

The “Pentagon” store

Password recovery

How your dog Max threatens your identity

What happens when you forget your password?

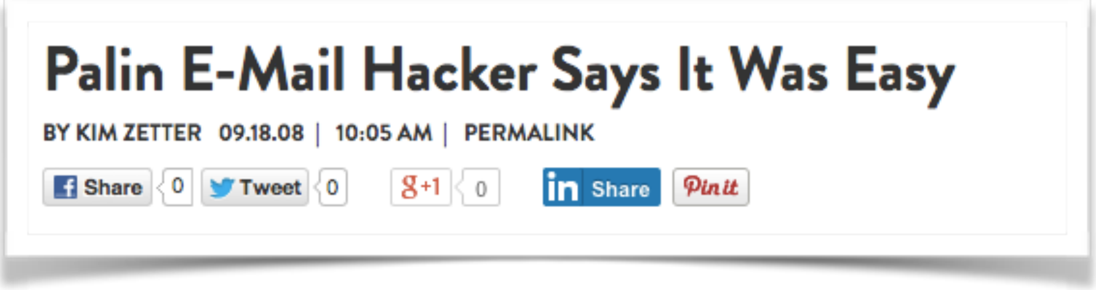
Two popular recovery mechanisms:

- E-mail
  - Risks exemplified by Mat Honan’s story
- Personal questions
  - Also called “security questions,” “personal knowledge questions,” or “life questions”
  - Another something-you-know factor

Sarah Palin's password recovery

- On 16 Sept. 2008, then Gov. Palin's Yahoo! account was hacked. How?
- Password reset
  - Zip code?
    - Only 2 in Wasilla
  - Date of birth?
    - Wikipedia: February 11, 1964
  - Where did you meet your spouse?
    - Wikipedia: met Todd in high school…
- Password posted to /b/ on 4chan.
- When everyone tried to log into Palin's account, Yahoo! finally detected attack
- 20-year-old hacker David Kernell (a.k.a. Rubico) caught
  - Sentenced to one year of federal prison

Sarah Palin's identity theft problem



Palin E-Mail Hacker Says It Was Easy

BY KIM ZETTER 09.18.08 | 10:05 AM | PERMALINK

Problems with security questions

- What’s your high school mascot?
- Name of favorite elementary school teacher?
- Name of college you applied to but did not attend?
- Who is your favorite president? What is your favorite color?

(Um, is it Calvin Coolidge?)

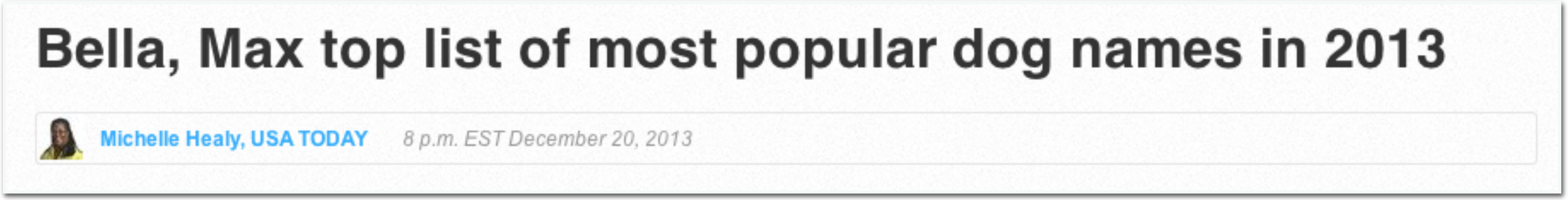
[illegible]

- Which college did you attend?

Source: A. Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of Facebook. SOUPS 2008.

Answers easy to guess or find out…

- Name of your first / favorite pet?



Bella, Max top list of most popular dog names in 2013

Michelle Healy, USA TODAY *8 p.m. EST December 20, 2013*

- First name of your best friend?
    - 10% of men: James/Jim, John, Robert/Bob/Rob
- Top 500 names achieve 65% coverage
- Information available from Facebook, etc.
    - Where you went to school, college athletic rivals, favorite book/movie/pastime, high school mascot

or hard to remember…

- Name of the street you grew up on?
  - There can be more than one.
- Name of your best friend?
  - Depends on my mood.
- City where you were born?
  - NYC? New York? Manhattan? New York City? Big Apple?
- People lie to increase security… then forget their answers.

Slide source: V. Shmatikov, 2014

HealthCare.gov

Federal:

- What is a relative's telephone number that is not your own?
- Type a significant date in your life?
- What is the name of the manager at your first job?

Individual states:

- What is your youngest child's birth weight?
- What color was your first bicycle?
- If you needed a new first name, what would it be?
- What band poster did you have on your wall in high school?
- How many bones have you broken?

One password defense:
Expiration

Password expiration

- Common interval: 90 days
- May help sometimes, but…
  - Helps users forget passwords
    - Estimated $150 cost per user per year
      - META group estimate: 1.75 help desk calls a month; Gartner group: 30% of calls are for password resets; Forester research: $25 / call
  - Makes social engineering *worse*

8 glasses of water / day
and 90 days between password
resets

Password expiration

How do users change their passwords?

```
Password1

Password2

Password3

Pa$sword1
```

Password expiration

UNC Experiment:

- Obtained password hashes (MD5, no salt) from 10374 defunct UNC accounts
- Cracked password other than last one in 7752 accounts
  - Call these "eligible" accounts
- Defined set T(*P*) of transformations ("tweaks") on password *P*
  - E.g., `s' <- '$' (LEET), '1' <- '2', etc.
- Given cracked password, found future password in T(*P*) for 41% of eligible accounts
  - Most effective algorithm tried expected 481607.44 elements of T(*P*)

- Y. Zhang, F. Monrose, M. K. Reiter: The security of modern password expiration: an al

Password managers to the rescue!

Password managers

- Why should users have to remember passwords?
- Password managers solve this problem.
  - LastPass, RoboForm, Dashlane, KeePass, etc.

dashlane

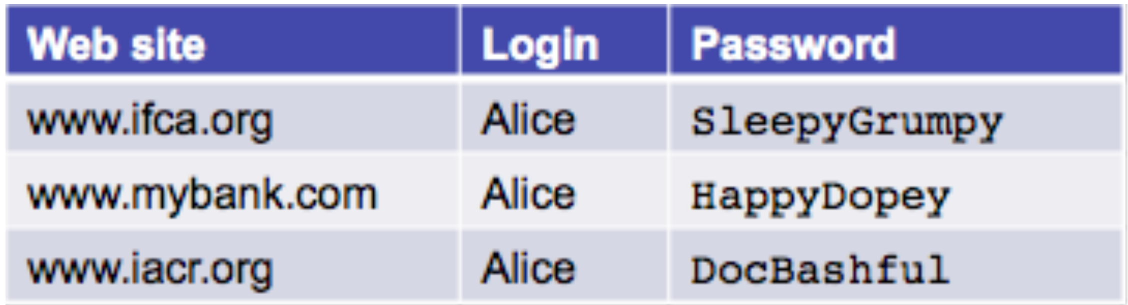
KeePass

LastPass ****

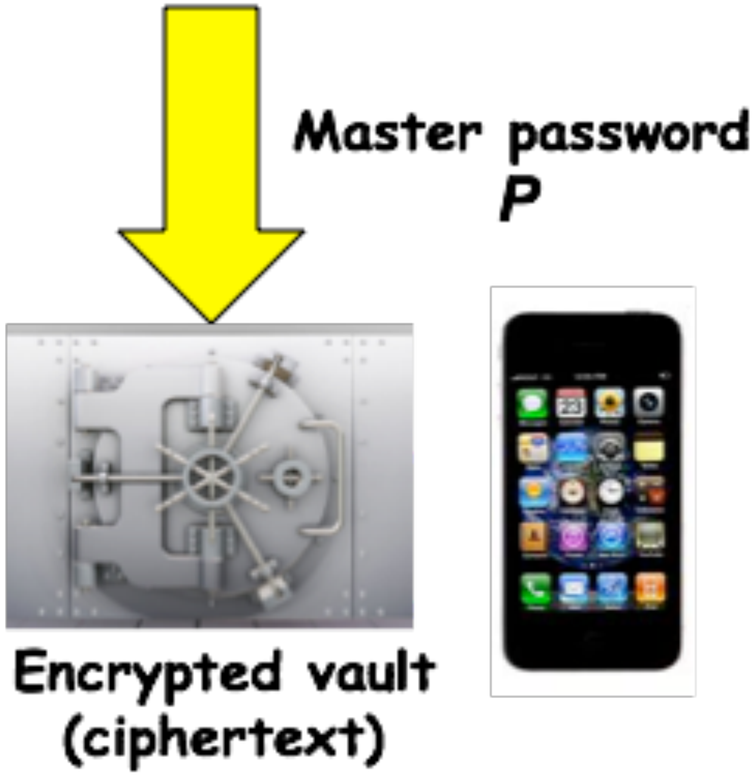
The Last Password You'll Ever Need.

Password managers

- Idea: Encrypt all of your passwords under a single, *master password*
- One password to rule them all…

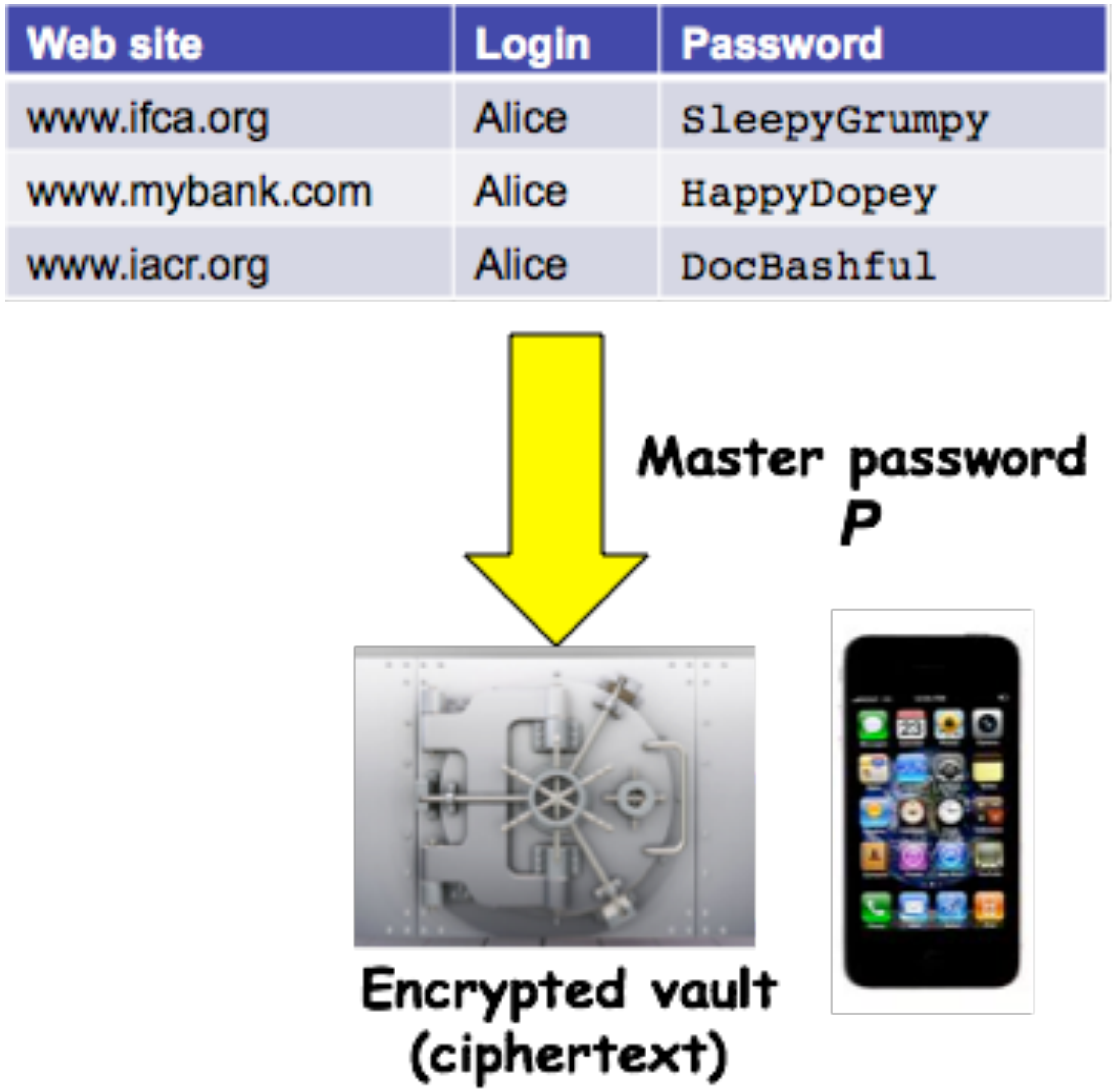


Web site	Login	Password
www.ifca.org	Alice	SleepyGrumpy
www.mybank.com	Alice	HappyDopey
www.iacr.org	Alice	DocBashful



Password managers

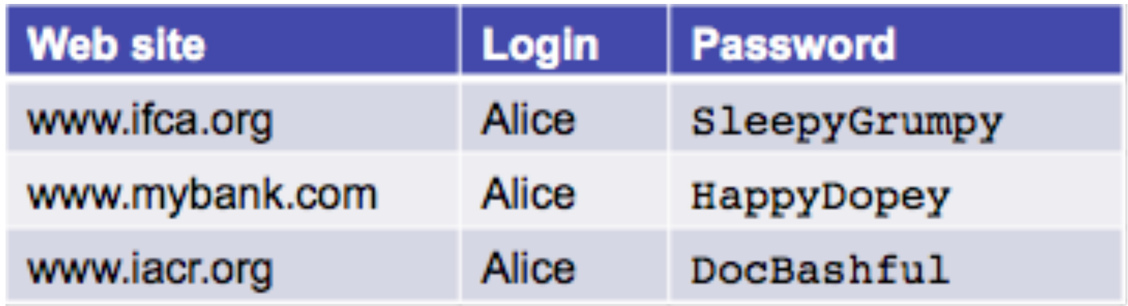
- The good:
  - Vault makes it easy to use strong passwords
  - E.g., automatically generated passwords
    - See `lastpass.com/generatepassword.php`
      - Passwords like "1UjCQMd8d0"



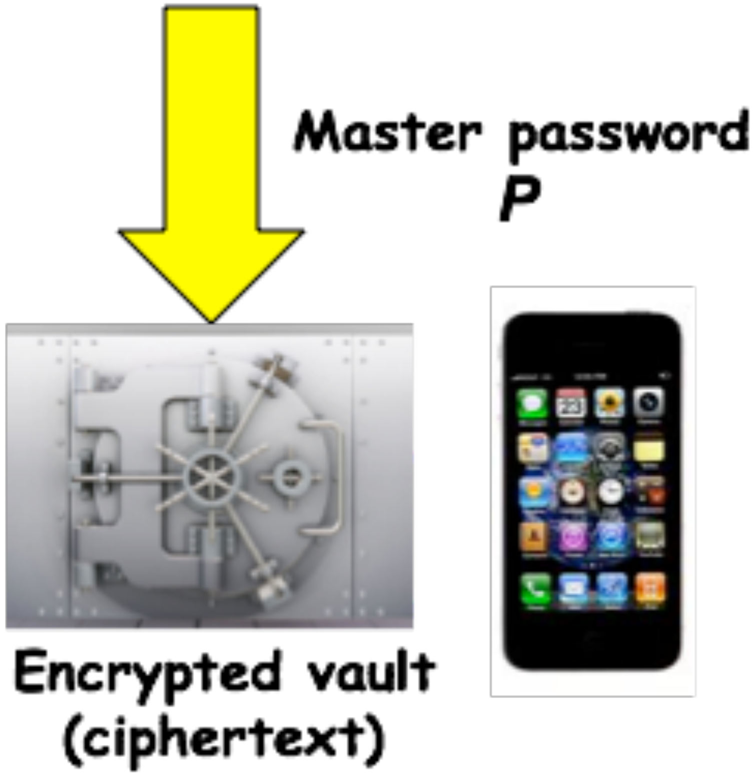
Web site	Login	Password
www.ifca.org	Alice	`SleepyGrumpy`
www.mybank.com	Alice	`HappyDopey`
www.iacr.org	Alice	`DocBashful`

Password managers

- The bad
  - Why might a master password be weaker than an ordinary one?
    - You have to type it *often*
    - You often have to type it on a mobile device
  - How is a master password cracked?
    - Slight modification of John the Ripper, etc.

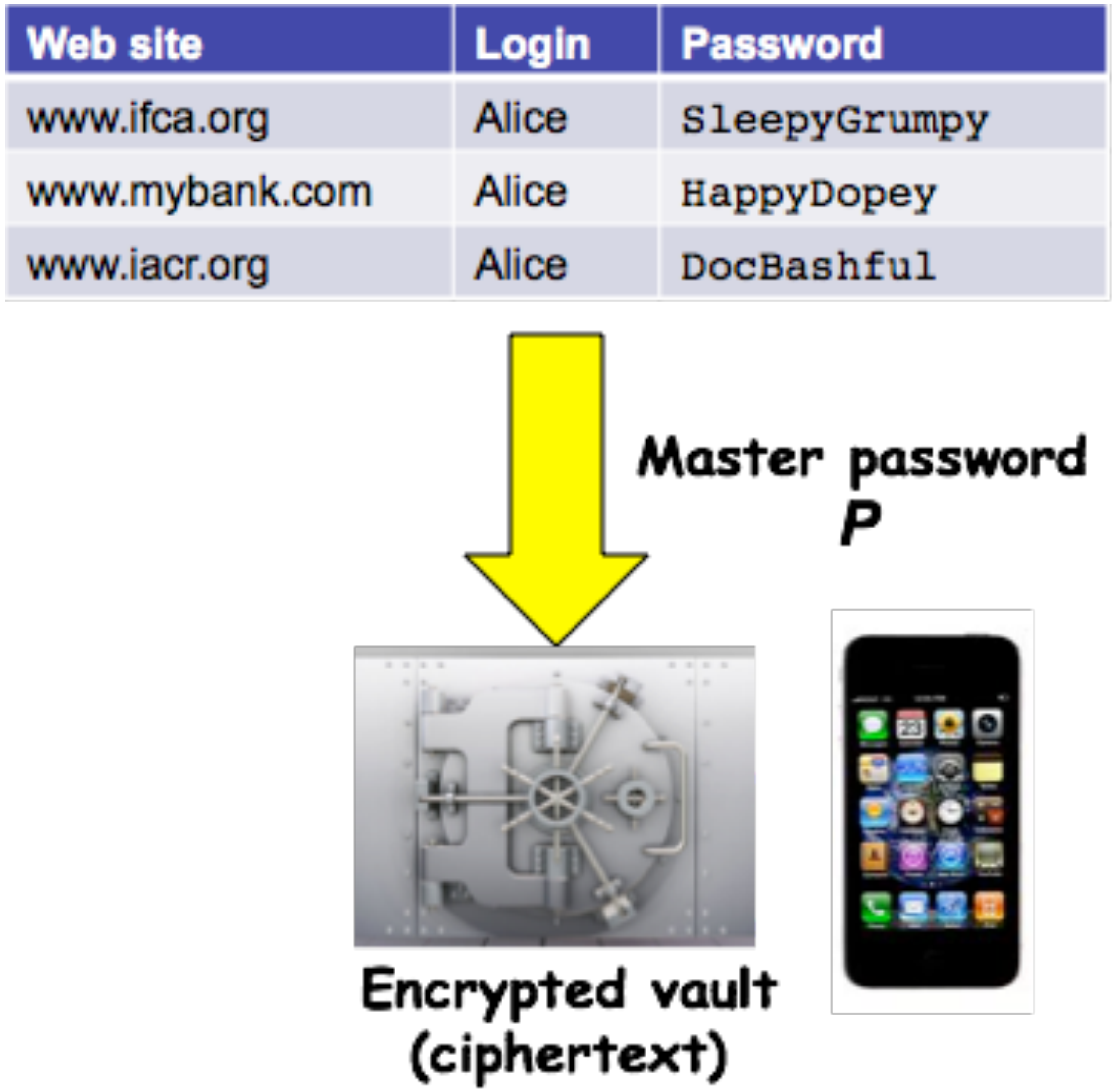


Web site	Login	Password
www.ifca.org	Alice	`SleepyGrumpy`
www.mybank.com	Alice	`HappyDopey`
www.iacr.org	Alice	`DocBashful`



Password managers

- The ugly
  - Password vaults backed up in cloud
  - *Effectively protected only by master password*
  - Why? Synchronization / recovery
  - What does this mean?
    - Bad master password ☞ all your vault passwords vulnerable to cracking attack



Web site	Login	Password
www.ifca.org	Alice	SleepyGrumpy
www.mybank.com	Alice	HappyDopey
www.iacr.org	Alice	DocBashful

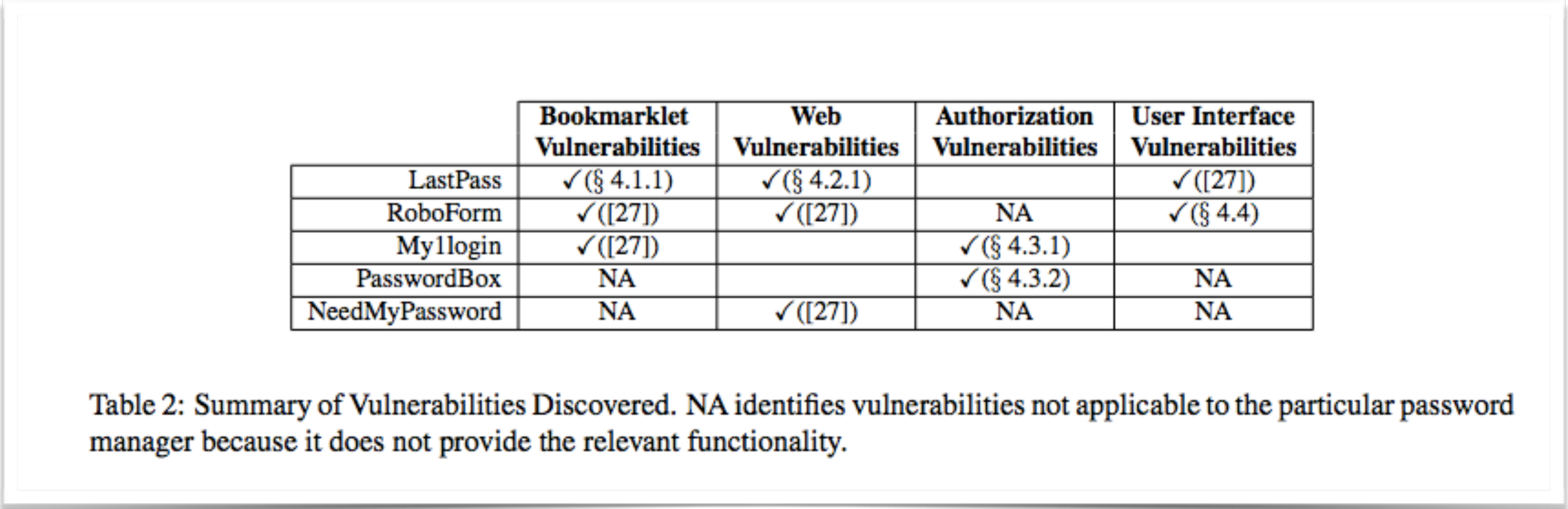
Password managers

- The ugly
  - Of course, password management services are a nice target for hacking
  - LastPass has been breached *twice!*
  - 2011: LastPass asks users to change master passwords
  - 2015: "LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised"

How long will your password last?

Implementation issues

- Password vaults can be buggy—like any other software.
- Recent study found serious vulnerabilities in five popular managers
  - Z. Li, W. He, D. Akhawe, D. Song. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, 2014
- Analyzed five popular password managers



	Bookmarklet Vulnerabilities	Web Vulnerabilities	Authorization Vulnerabilities	User Interface Vulnerabilities
LastPass	✓(§ 4.1.1)	✓(§ 4.2.1)		✓([27])
RoboForm	✓([27])	✓([27])	NA	✓(§ 4.4)
My1login	✓([27])		✓(§ 4.3.1)	
PasswordBox	NA		✓(§ 4.3.2)	NA
NeedMyPassword	NA	✓([27])	NA	NA

Table 2: Summary of Vulnerabilities Discovered. NA identifies vulnerabilities not applicable to the particular password manager because it does not provide the relevant functionality.

The New York Times Magazine

The Secret Life of Passwords

We despise them – yet we imbue them with our hopes and dreams, our dearest memories, our deepest meanings. They unlock much more than our accounts.

By IAN URBINA   Video by LESLYE DAVIS

- Passwords are very interesting anthropological artifact!
- Keepsake passwords… ritualize a daily encounter with personal memories"
  - "Fiona Moriarty, a competitive runner… often used “16:59” — her target time for the 5,000 meters in track"
  - "To help quell his anger at his ex-wife soon after their divorce, Estrella had reset his password to “Forgive@h3r.”
  - "[H]e moved on to other goals: “Quit@smoking4ever” (successful); “Save4trip@thailand” (successful); “Eat2@day” (“it never worked, I’m still fat,” Estrella wrote); “Facetime2mom@sunday” (“it worked,” he said, “I’ve started talking with my mom every week now”)."

Source: http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html

Lecture takeaways

User authentication is a mess because of…

- Weak secrets
  - Users choose weak passwords or…

    they don't change defaults or…

    they give passwords away for candy.
  - "Life questions" encourage weak answers—or forgettable ones.
  - Guessing probability GP (or min-entropy) is a key measure of strength.
- Password cracking
  - Password hashes can be "cracked" when passwords are weak.
- Password managers are a good idea, but need work.