CS 361S

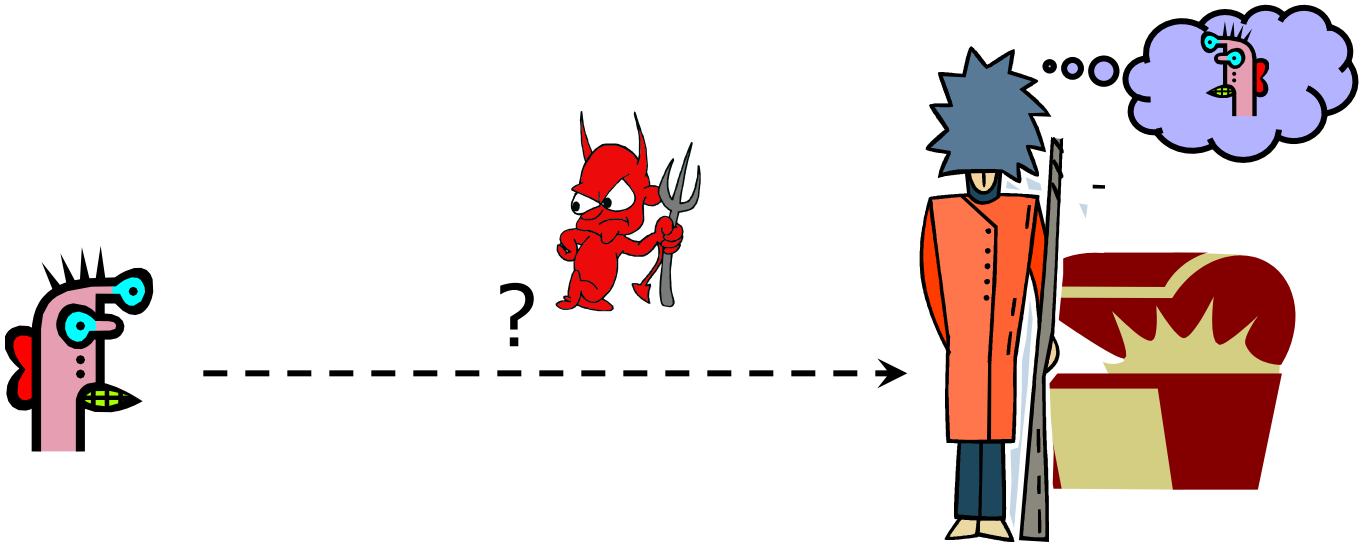
Authentication: Passwords and Security Questions

Vitaly Shmatikov

Reading Assignment

- Read Kaufman 9.1-2, 10.1-10, 11.1-2, 12.2
  - Don’t have to read about public-key authentication (yet)

Basic Problem



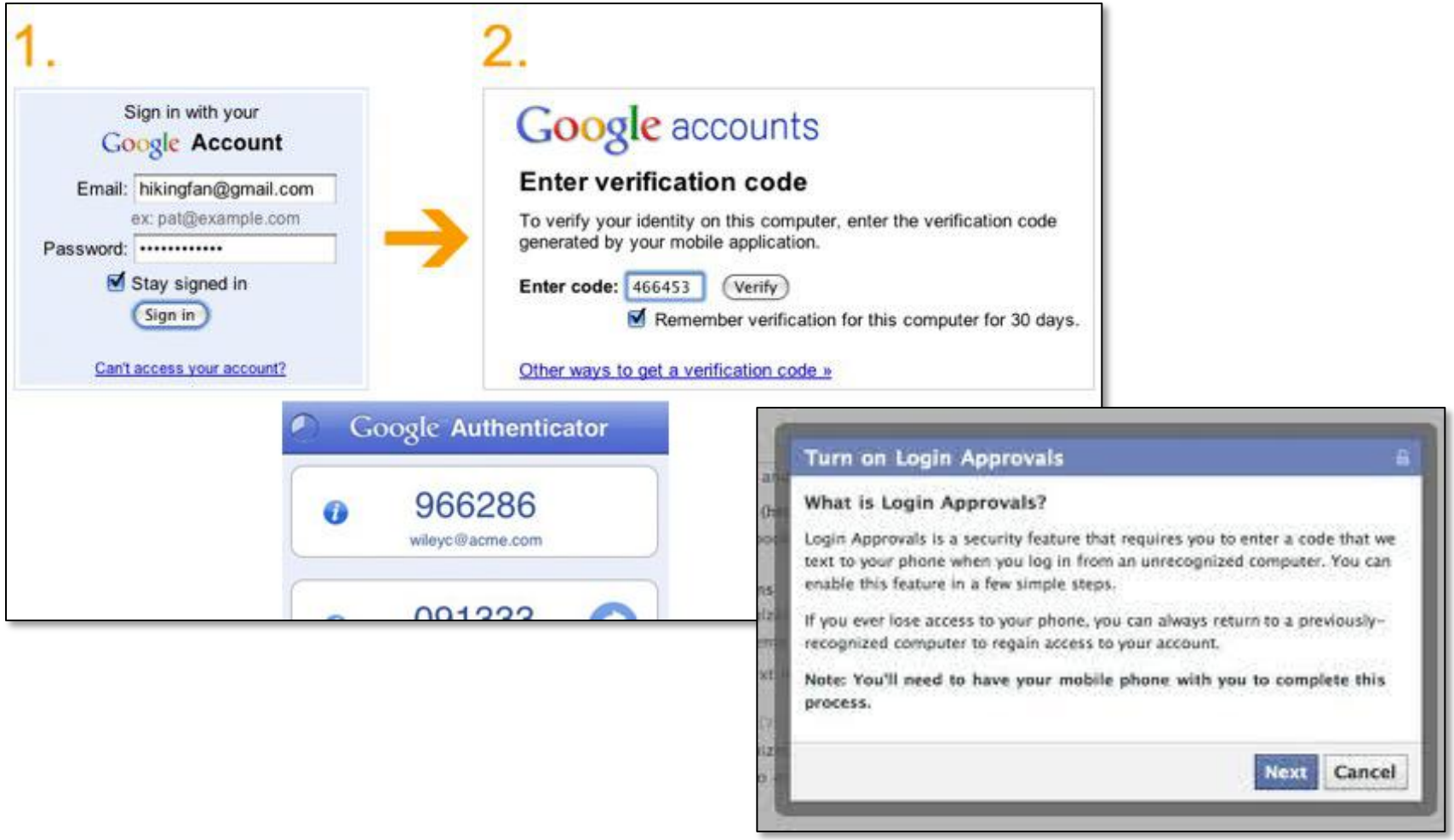
How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem

Many Ways to Prove Who You Are

- What you know
  - Passwords
  - Answers to questions that only you know
- Where you are
  - IP address, geolocation
- What you are
  - Biometrics
- What you have
  - Secure tokens, mobile devices

Multi-Factor Authentication



Password-Based Authentication

User has a secret password.

System checks it to authenticate the user.

- How is the password communicated?
  - Eavesdropping risk
- How is the password stored?
  - In the clear? Encrypted? Hashed?
- How does the system check the password?
- How easy is it to guess the password?
  - Easy-to-remember passwords tend to be easy to guess

Other Aspects

- Usability
  - Hard-to-remember passwords?
  - Carry a physical object all the time?
- Denial of service
  - Stolen wallet
  - Attacker tries to authenticate as you, account locked after three failures
  - "Suspicious" credit card usage
- Social engineering

Passwords and Computer Security

- In 2012, 76% of network intrusions exploited weak or stolen credentials (username/password)
  - Source: Verizon Data Breach Investigations Report
- First step after any successful intrusion: install sniffer or keylogger to steal more passwords
- Second step: run cracking tools on password files
  - Cracking needed because modern systems usually do not store passwords in the clear (how are they stored?)
- In Mitnick's "Art of Intrusion", 8 out of 9 exploits involve password stealing and/or cracking

Password Security Risks

- Keystroke loggers
  - Hardware
    - KeyGhost, KeyShark, others
  - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
  - TENEX timing attack
- Social engineering

Default Passwords

- Pennsylvania ice cream shop phone scam
  - Voicemail PIN defaults to last 4 digits of phone number; criminals change message to "I accept collect call", make $8600 on a 35-hour call to Saudi Arabia
- Examples from Mitnick's "Art of Intrusion"
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
  - "Dixie bank": break into router (pwd="administrator"), then into IBM AS/400 server (pwd="administrator"), install keylogger to snarf other passwords
    - "99% of people there used 'password123' as their password"

Gary McKinnon

- Scottish "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

Old Password Surveys

- Klein (1990) and Spafford (1992)
  - 2.7% guessed in 15 minutes, 21% in a week
  - Much more computing power is available now!
- U. of Michigan: 5% of passwords were "goblue"
  - How many passwords on this campus involve "orange", "horns", "bevo", etc.?
- Zviran and Haga (1999)
  - Password usage at a DoD facility in California
  - 80% of passwords were 4-7 characters in length, 80% used alphabetic characters only, 80% of the users had never changed their password

rockyou™ Hack (2009)

- "Social gaming" company
- Database with 32 million user passwords from partner social networks
- Passwords stored in the clear
- December 2009: entire database hacked using an SQL injection attack and posted on the Internet
  - More about SQL injection attacks later

Passwords in RockYou Database

[Imperva]

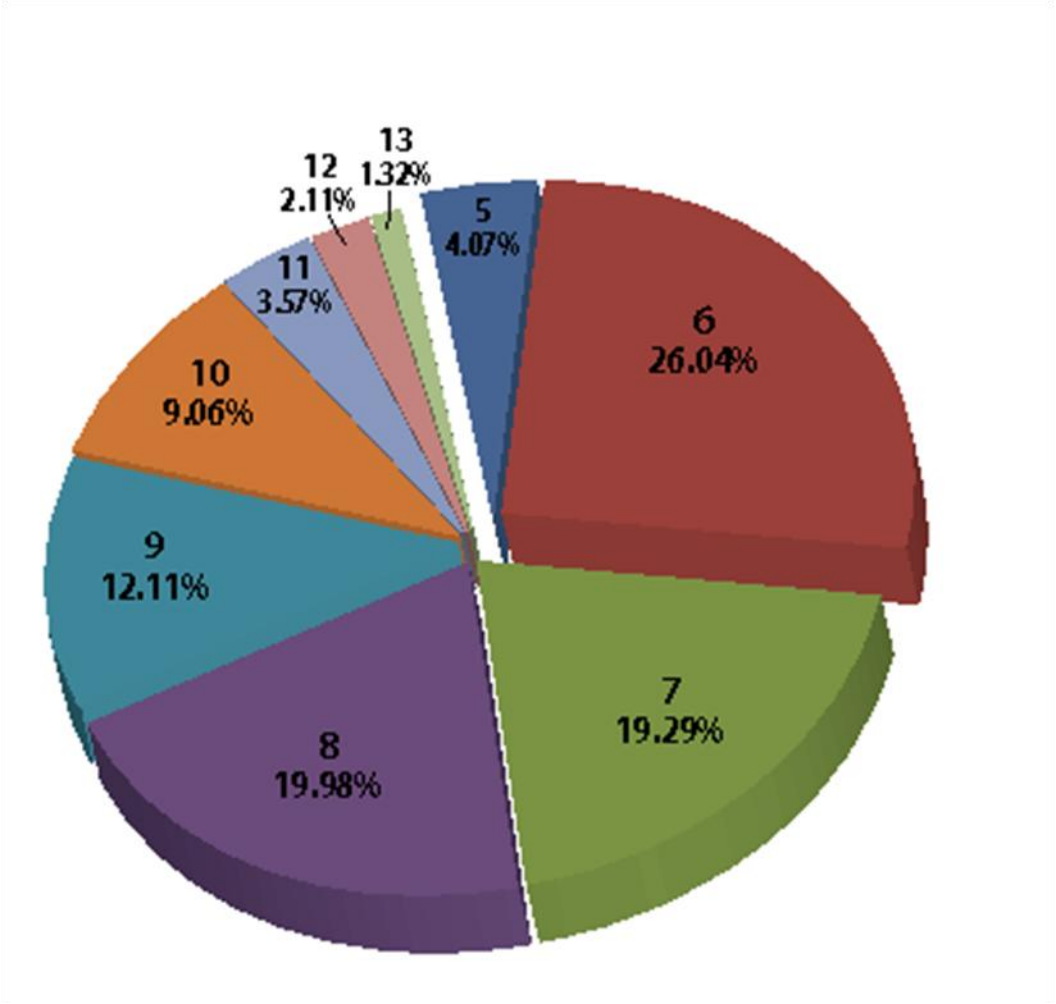
Password Popularity – Top 20

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

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

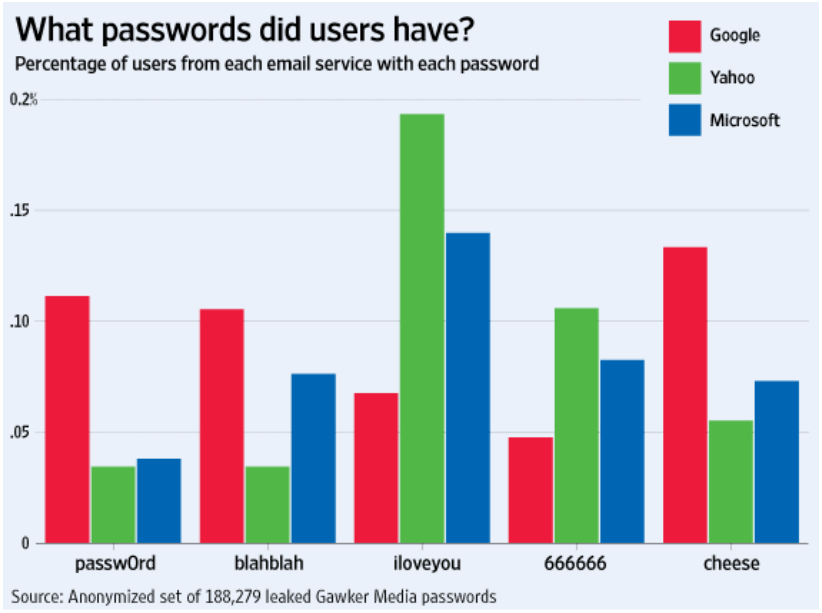
Password Length Distribution

[Imperva]



Gawker Passwords (2010)

[WSJ]



Stratfor Passwords (2011)

- Austin forecasting and intelligence firm
- Hacked on December 24, 2011
  - Client names, credit card numbers (in the clear, with CVV!), 860,000 MD5-hashed passwords
- 86% of password hashes recovered by Gerrit Padgham using GPU technology
  - Many very weak passwords
    - Top ten: stratfor, 123456, 0000, password, stratfor1, changeme, strat4, 1qaz2wsx, 1234, wright
  - 630,000 algorithmically generated by Stratfor
    - 8 characters, mixed uppercase & lowercase, digits

More Password Datasets

PlentyOfFish® Free Online Dating

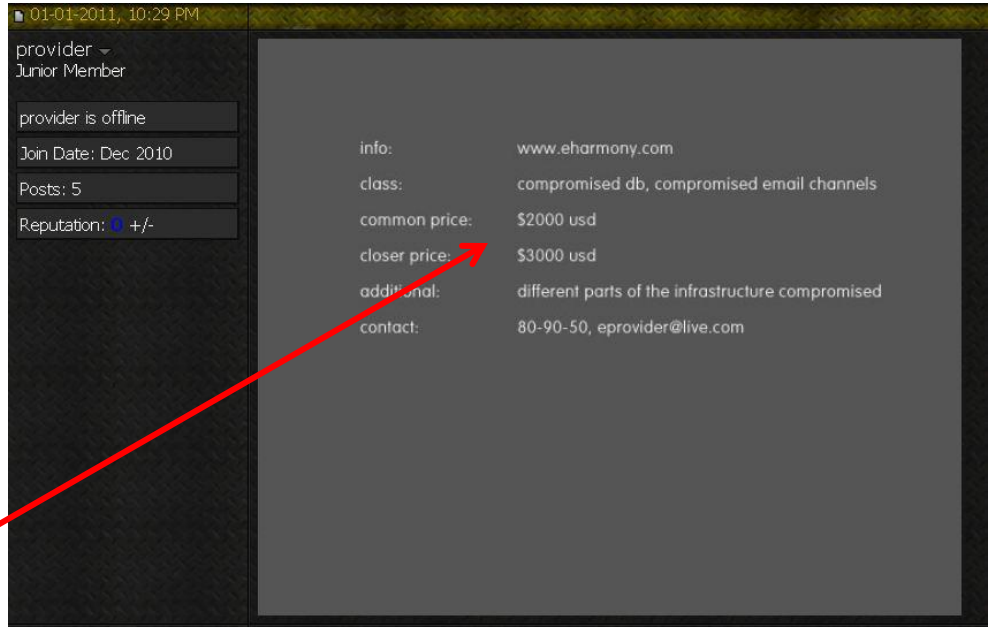
More than 30 million passwords

eHarmony®

"#1 Most Trusted Online Dating Site"

SQL injection attack

For sale for $3000



Adobe Passwords (2013)

- 153 million account passwords
  - 56 million of them unique
- Encrypted using 3DES in ECB mode rather than hashed (why is this important?)

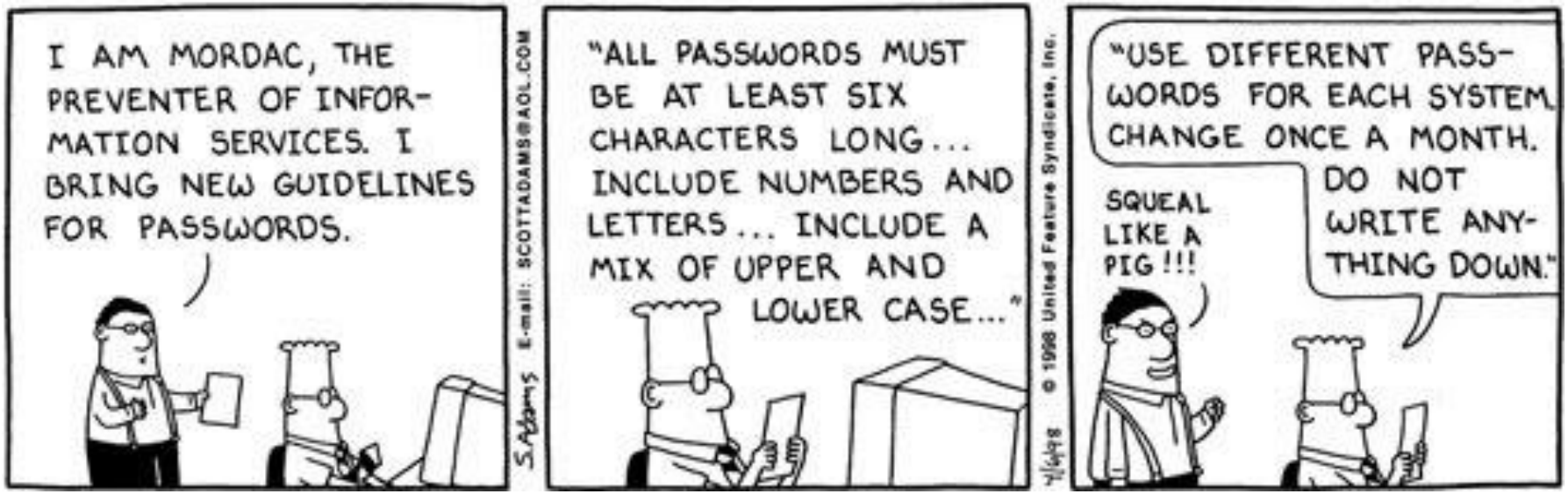
How About PINs?

- In 2012, Nick Berry analyzed all four-digit passwords from previous leaks

	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%

	PIN	Freq
#9980	8557	0.001191%
#9981	9047	0.001161%
#9982	8438	0.001161%
#9983	0439	0.001161%
#9984	9539	0.001161%
#9985	8196	0.001131%
#9986	7063	0.001131%
#9987	6093	0.001131%
#9988	6827	0.001101%
#9989	7394	0.001101%
#9990	0859	0.001072%
#9991	8957	0.001042%
#9992	9480	0.001042%
#9993	6793	0.001012%
#9994	8398	0.000982%
#9995	0738	0.000982%
#9996	7637	0.000953%
#9997	6835	0.000953%
#9998	9629	0.000953%
#9999	8093	0.000893%
#10000	8068	0.000744%

Password Usability



Memorability vs. Security

[Ross Anderson]

- One bank's idea for making PINs "memorable"
  - If PIN is 2256, write your favorite word in the grid

1	2	3	4	5	6	7	8	9	0
	b								
	l								
				u					
					e				

Normally 9,999 choices for PIN hard to guess

Now only a few dozen possible English words – easy to guess!

  - Fill the rest with random letters

Password Guessing Techniques

- Dictionary with words spelled backwards
- First and last names, streets, cities
- Same with upper-case initials
- All valid license plate numbers in your state
- Room numbers, telephone numbers, etc.
- Letter substitutions and other tricks
  - If you can think of it, attacker will, too

Social Engineering

- Univ. of Sydney study (1996)
  - 336 CS students emailed asking for their passwords
    - Pretext: "validate" password database after suspected break-in
  - 138 returned their passwords; 30 returned invalid passwords; 200 reset passwords (not disjoint)
- Treasury Dept. report (2005)
  - Auditors pose as IT personnel attempting to correct a "network problem"
  - 35 of 100 IRS managers and employees provide their usernames and change passwords to a known value
- Other examples: Mitnick's "Art of Deception"

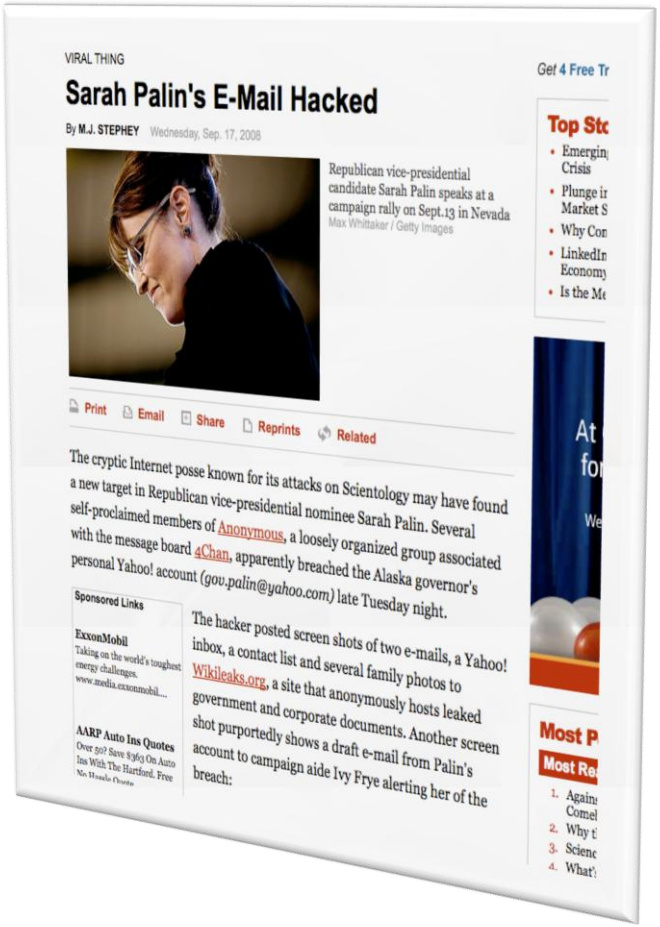
How People Use Passwords

- Write them down
- Use a single password at multiple sites
  - Do you use the same password for Amazon and your bank account? UT Direct? Do you remember them all?
- Forget them… many services use "security questions" to reset passwords
  - "What is your favorite pet's name?"
  - Paris Hilton's T-Mobile cellphone hack

Sara Palin's Email Hack

[slide: Gustav Rydstedt]

- Reset password for **gov.palin@yahoo.com**
  - No secondary email needed
  - Date of birth? Wikipedia
  - ZIP code? Wasilla has 2
  - Where did you meet your spouse? Wikipedia, Google, …
- Changed pwd to "popcorn"
- Hacker sentenced to
  1 year in prison +
  3 yrs of supervised release


VIRAL THING

Sarah Palin's E-Mail Hacked

By M.J. STEPHEY Wednesday, Sep. 17, 2008

Republican vice-presidential candidate Sarah Palin speaks at a campaign rally on Sept.13 in Nevada

Max Whittaker / Getty Images

Print Email Share Reprints Related

The cryptic Internet posse known for its attacks on Scientology may have found a new target in Republican vice-presidential nominee Sarah Palin. Several self-proclaimed members of Anonymous, a loosely organized group associated with the message board 4Chan, apparently breached the Alaska governor's personal Yahoo! account (gov.palin@yahoo.com) late Tuesday night.

The hacker posted screen shots of two e-mails, a Yahoo! inbox, a contact list and several family photos to Wikileaks.org, a site that anonymously hosts leaked government and corporate documents. Another screen shot purportedly shows a draft e-mail from Palin's account to campaign aide Ivy Frye alerting her of the breach:

Sponsored Links

ExxonMobil

AARP Auto Ins Quotes

Top Stc

Most P

Twitter Hack (1)

- In 2009, "Hacker Croll" downloaded and posted 310 internal Twitter documents
- Step 1: 0wn email account of a Twitter employee
  - Answer "security question," system sends password reset link to secondary email: ******@h******.com
    - Guess hotmail.com, guess username from public information
  - Hotmail.com account no longer active - register it, get reset link, reset password
  - Analyze old email messages to learn original password
    - For example, lost password messages from other Web services
  - Restore password to original so owner doesn't notice

Twitter Hack (2)

- Step 2: use found password to log into Twitter employee's work account on Google Apps
  - Download internal Twitter documents
- Step 3: rinse and repeat
  - Same username/password combination and password reset features to access AT&T, Amazon, iTunes
  - iTunes reveals credit card info in the clear

Problems with Security Questions

[Rabkin, "Security questions in the era of Facebook"]

- Inapplicable
  - What high school did your spouse attend?
- Not memorable
  - Name of kindergarten teacher? Price of your first car?
- Ambiguous
  - Name of college you applied to but did not attend?
- Easily guessable
  - Age when you married? Year you met your spouse? Favorite president? Favorite color?
- Automatically attackable (using public records!)

Answers Are Easy to Find Out…

- Make of your first car?
  - Until 1998, Ford had >25% of market
- First name of your best friend?
  - 10% of males: James/Jim, John, Robert/Bob/Rob
- Name of your first / favorite pet?
  - Max, Jake, Buddy, Bear…
  - Top 500 (covers 65% of names) available online
- Information available from Facebook, etc.
  - Where you went to school, college athletic rivals, favorite book/movie/pastime, high school mascot

…or Easy to Forget

- Name of the street, etc.
  - More than one
- Name of best friend
  - Friends change
- City where you were born?
  - NYC? New York? Manhattan? New York City? Big Apple?
- People lie to increase security… then forget the answers

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?

Guessing Mother's Maiden Name

[Griffith and Jakobsson]

- Griffith and Jakobsson, "Messin' with Texas: Deriving Mother's Maiden Names Using Public Records" (2005)
- Insight: MMN is a fact, not a secret
- Figure out people's MMN by creating ancestry trees from records that are public by law
- Target: Texas
  - Large population
  - Close to national averages
  - Good online records

Useful Public Records (1)

[Griffith and Jakobsson]

- US Census records
  - Individual records released with 72-year delay
    - Individual data sheets for the 1940 Census released in 2012
  - Can read MMN directly, but difficult
- Voter registration records
  - 67% of Texans registered to vote (2000)
  - Voter information has "Other Name" field, people often put maiden name there
  - Also full name, date of birth, address
  - Not free!

Useful Public Records (2)

[Griffith and Jakobsson]

- Property records
  - Match addresses to names ("legally enforced phonebooks"), good in combination with phonebooks
  - Include people who have children but haven't married
- Obituaries
  - Obituaries of "important" people in local newspapers often mention spouse, children, date of birth, when married, etc.
- SSDI (Social Security Death Index)
  - Free, comprehensive, but no direct MMN info
  - Purpose: prevent mafia from using SSNs of dead people

Useful Public Records (3)

[Griffith and Jakobsson]

- Marriage records
  - Names and ages of bride and groom, date of marriage, where married
- Birth records
  - Full name, date of birth, where born
- Sources of birth and marriage records
  - Mormons
  - Rootsweb.com's WorldConnect
    - Family trees for 4499 living Texans
  - Rootsweb.com's USGenWeb
    - 11,358,866 birth records, mainly from county records

Texas Bureau of Vital Statistics

[Griffith and Jakobsson]

- 1966-2002 marriage index online
- 1968-2002 divorce index online

- 1926-1995 birth records, taken offline in 2000
  - So that adopted children can't find their natural parents
  - Copies still available at archive.org
- 1965-1999 death records, taken offline in 2002
  - Unlinked, but actual files still found at old URLs

Low-Hanging Fruit in Birth Records

[Griffith and Jakobsson]

- 1923-1949 birth records have MMN in plaintext
  - 1,114,680 males auto-compromised
- 1,069,448 females in records
  - Linking females born in 1923-1949 to marriages 1966-2002 gives 288,751 compromises (~27%)
    - Use full name, DoB to connect women to marriages
    - If more than 1 marriage per woman, divorce records help
- 1950-1995 has 40,697 hyphenated last names

Insights for Guessing MMN

[Griffith and Jakobsson]

- Children have same last name as their parents
- Suffixed children will have same first and last name as parents
- Children often born shortly after parents' marriage
- Children born shortly after parents' marriage often born in same county
  - Makes guessing much easier than you'd normally think... Especially true for the clustering of names within ethnic groups - don't have to pick the correct parents, just the correct MMN!

Example #1: Unique Last Name

[slide: Virgil Griffith]

Ernest AAKQUANAHANN

Dionne COX

Mother's maiden name = COX

Example #2: Two Marriages

[slide: Virgil Griffith]

Shawn ZUTTER

Lisa MENDOZA

Chad ZUTTER

Lauren LANDGREBE

Entropy = 1 bit

(need at most 2 guesses)

Example #3: Two Marriages

[slide: Virgil Griffith]

Robert STUGON

Duarte STURNER

Jim STUGON

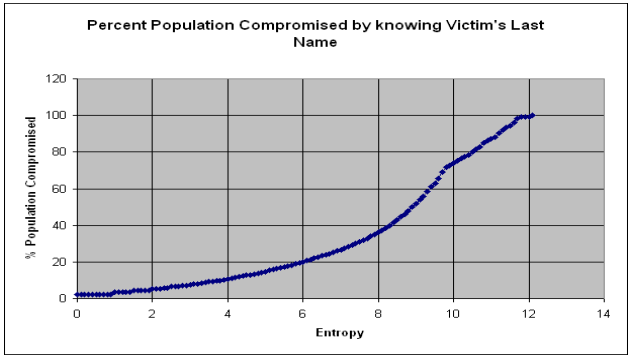
Luann STURNER

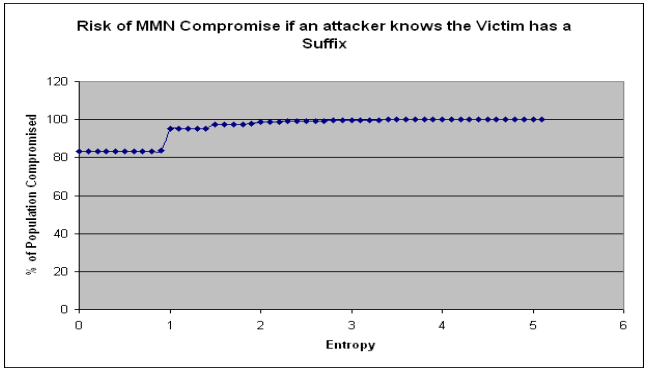
Mother's maiden name = STURNER

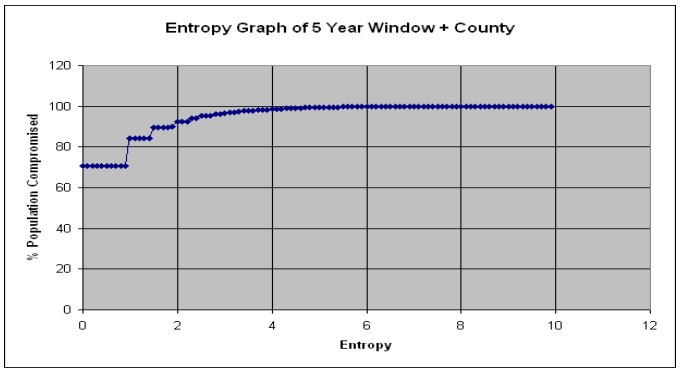
Insights for Guessing MMN

[Griffith and Jakobsson]

- Last names + birth records
  + 82,272 Texans
    - Birth records not very comprehensive
- Suffixed last names
  + 344,463 Texans
    - 60% of suffixed children in birth records
- Assume child is born 5 years from marriage, in the same county
  + 2,355,828 Texans



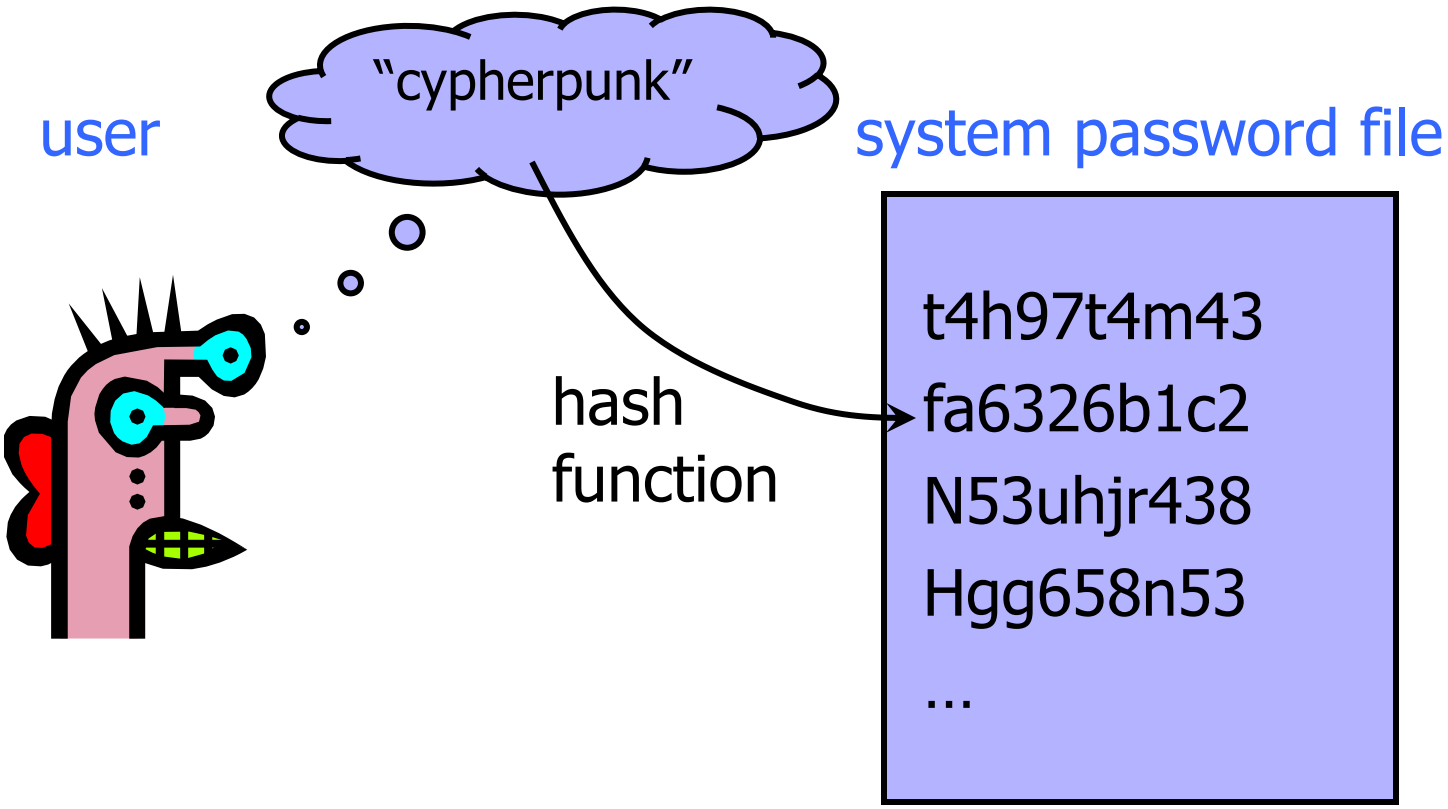




MMN Considered Harmful

- Griffith-Jakobsson study figured out mother's maiden name for 4,190,493 Texans using only free, public sources of information
  - 1/5 of the state's population
- More sources of information available
  - More comprehensive birth records available for sale
- More sophisticated analyses possible
- Conclusion: mother's maiden name is not a secure authentication factor

Storing Passwords



Password Hashing

- Instead of user password, store Hash(password)
- When user enters a password, compute its hash and compare with the entry in the password file
  - System does not store actual passwords
  - Cannot go from hash to password
    - … except by guessing the password
- Hash function H must have some properties
  - Given H(password), hard to find any string X such that H(X)=H(password) - why?

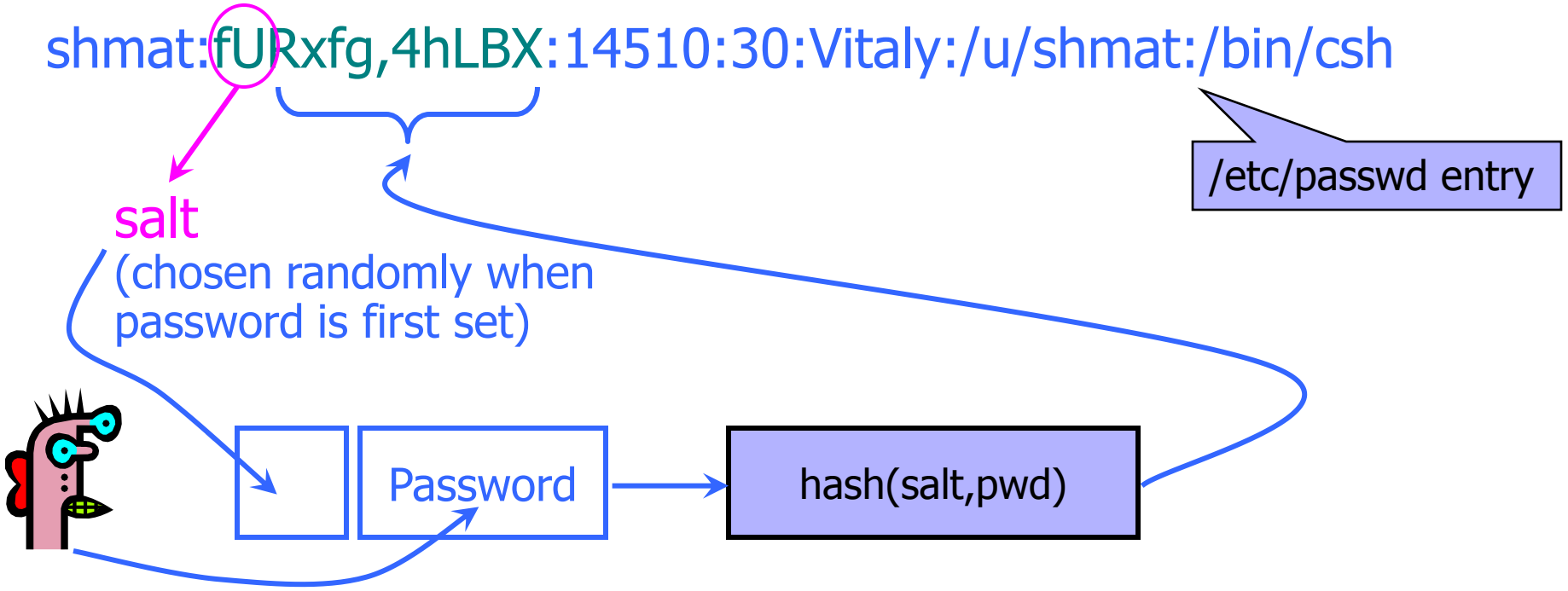
UNIX Password System

- Uses DES encryption as if it were a hash function
  - Encrypt NULL string using the password as the key
    - Truncates passwords to 8 characters!
  - Artificial slowdown: run DES 25 times (why?)
  - Can instruct modern UNIXes to use MD5 hash function
- Problem: passwords are not random
  - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are $94^8 \approx 6$ quadrillion possible 8-character passwords
  - Humans like to use dictionary words, human and pet names $\approx$ 1 million common passwords

Dictionary Attacks

- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can pre-compute H(word) for every word in the dictionary – this only needs to be done once!
    - This is an offline attack
    - Once password file is obtained, cracking is instantaneous
  - Sophisticated password guessing tools are available
    - Take into account frequency of letters, password patterns, etc.
- In UNIX, /etc/passwd is world-readable
  - Contains user IDs and group IDs which are used by many system programs

Salt

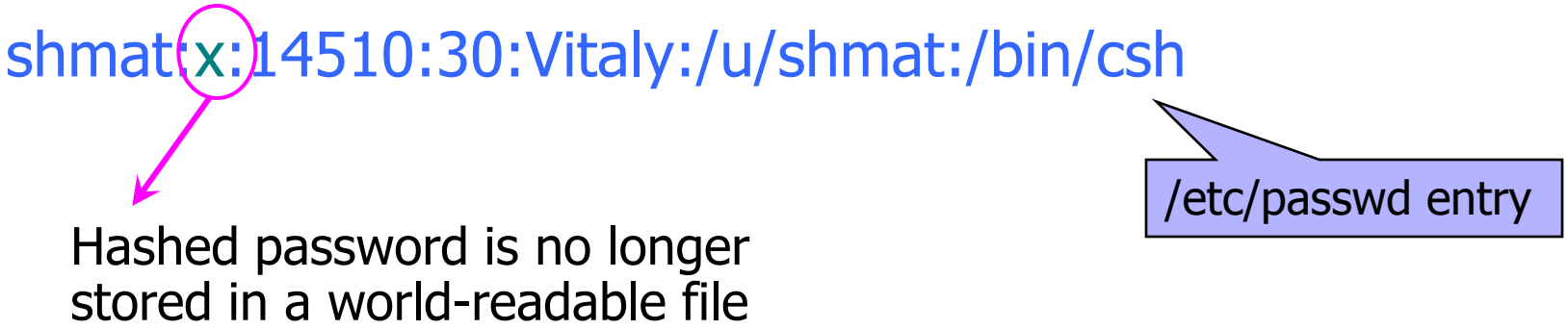


- Users with the same password have different entries in the password file
- Offline dictionary attack becomes much harder

Advantages of Salting

- Without salt, attacker can pre-compute hashes of all common passwords once
  - Same hash function on all UNIX machines; identical passwords hash to identical values
  - One table of hash values works for all password files
- With salt, attacker must compute hashes of all common passwords for each possible salt value
  - With 12-bit random salt, the same password can hash to 4096 different hash values

Shadow Passwords



- Hashed passwords are stored in /etc/shadow file which is only readable by system administrator (root)
- Expiration dates for passwords
- Note: early Linux implementations of shadow called the login program which had a buffer overflow!

Password Hash Cracking

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

- Custom GPU-based hardware
  - A 5-server rig with 25 Radeon GPUs
  - 348 billion NTLM passwords per second
    - NTLM = Microsoft's suite of security protocols
    - 6 seconds to crack a 14-character Windows XP password
  - 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 - how?

Password Policies

[Inglesant and Sasse, "The True Cost of Unusable Password Policies"]

- Overly restrictive password policies…
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…
- … result in frustrated users and less security
  - Burdens of devising, learning, forgetting passwords
  - Users construct passwords insecurely, write them down
    - Can't use their favorite password construction techniques (small changes to old passwords, etc.)
    - "An item on my desk, then add a number to it"
  - Heavy password re-use across systems

Strengthening Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
  - Revocation is often a problem with biometrics
- Graphical passwords
  - Goal: increase the size of memorable password space
  - Dictionary attacks are believed to be difficult because images are very "random" - is this true?

Why Graphical Passwords?

- Idea: use a difficult AI problem
  - To authenticate a user, have him perform some easy task that would be hard for a computer algorithm
- Vision and image recognition are easy for humans, hard for machines
  - Faces are easy to remember and recognize
  - Images are easy to remember and recognize if accompanied by a memorable story
- Still some challenges
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

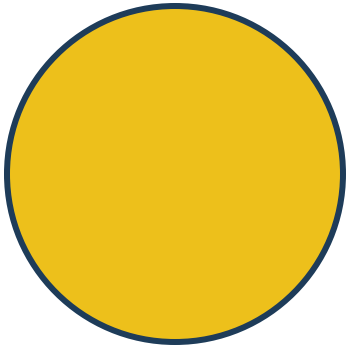
passfaces™
STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

Passfaces Meets the Challenge

Secure and Usable

The Brain Deals with Faces Differently than Any Other Image



Face recognition is a dedicated process which is different from general object recognition.

Source: Face Recognition: A Literature Survey. National Institute of Standards and Technology

Recall vs. Recognize

You must **RECALL** a password

You simply **RECOGNIZE** a face

Remember High School …. ***What kind of test did your prefer?***

Fill in the Blank

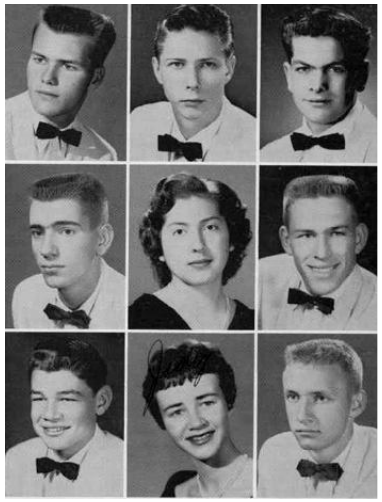
1 2 3 g f w y

Multiple Choice

We Never Forget a Face

Think about how many people you already recognize.

Why wouldn't you remember your Passfaces?



- *"Haven't used Passfaces in 6 months. I decided to take another look at it and, amazingly, I logged right in!"*
- *In one major government installation, there have been no forgotten Passfaces in over three years. The more its used, the easier it gets.*

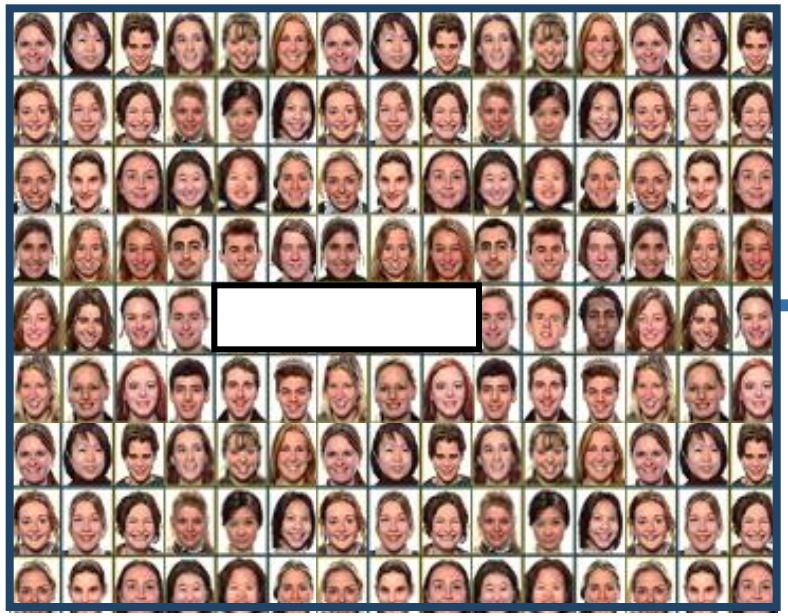
Our approach

Familiarize the user with a randomly-selected set of faces and check if they can recognize them when they see them again

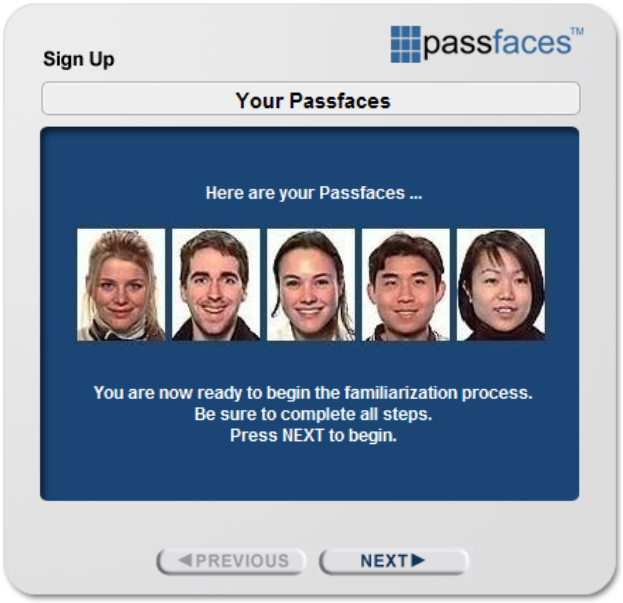
It's as easy as recognizing an old friend

How Passfaces Works

Library of Faces



User Interface

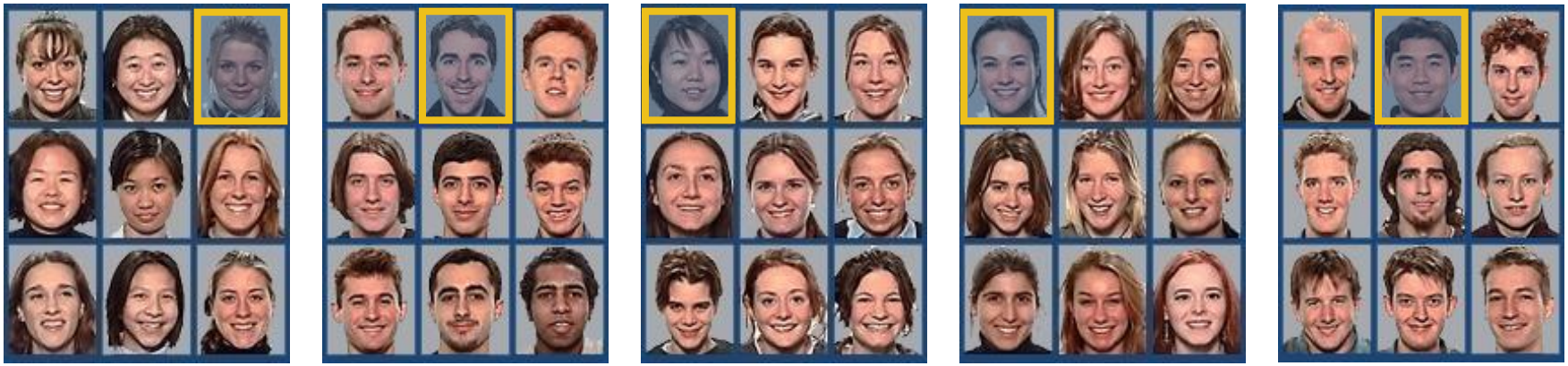


Users Are Assigned a Set of 5* Passfaces

* Typical implementation – 3 to 7 possible as standard

How Passfaces Works

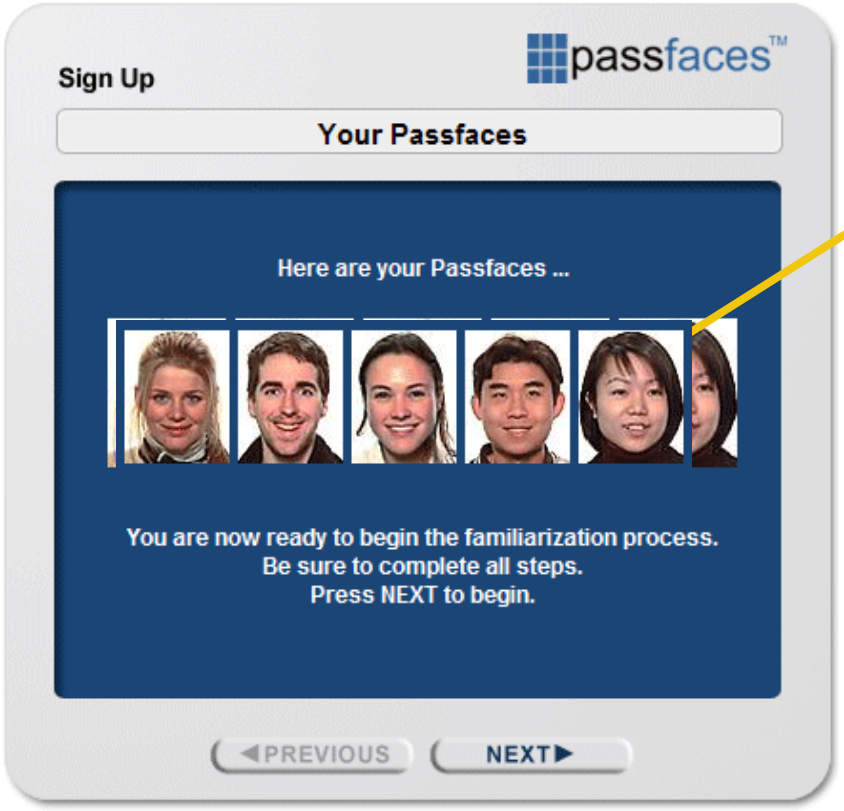
- 5 Passfaces are Associated with 40 associated decoys
- Passfaces are presented in five 3 by 3 matrices each having 1 Passface and 8 decoys



New Users are Familiarized with their Passfaces

- Users *enroll* with a 2 to 4 minute familiarization process
- Using instant feedback, encouragement, and simple dialogs, users are *trained* until they can easily recognize their Passfaces
- The process is optimized and presented like an easy game

Familiarization Puts Cookies in the Brain



Like a *mindprint* or *brain cookie*

But, unlike fingerprints,
Passfaces require no special hardware

And, unlike browser cookies,
Passfaces authenticate the actual user

A New Class of Authentication

- **Passfaces represents a new, 4th class of authentication:**

Cognometrics

Recognition-Based Authentication

Empirical Results

- Experimental study of 154 computer science students at Johns Hopkins and Carnegie Mellon
- Conclusions:
  - "… faces chosen by users are highly affected by the race of the user… the gender and attractiveness of the faces bias password choice… In the case of male users, we found this bias so severe that we do not believe it possible to make this scheme secure against an online attack…"
- 2 guesses enough for 10% of male users
- 8 guesses enough for 25% of male users

User Quotes

- "I chose the images of the ladies which appealed the most"
- "I simply picked the best lookin girl on each page"
- "In order to remember all the pictures for my login (after forgetting my 'password' 4 times in a row) I needed to pick pictures I could EASILY remember... So I chose beautiful women. The other option I would have chosen was handsome men, but the women are much more pleasing to look at"

More User Quotes

- "I picked her because she was female and Asian and being female and Asian, I thought I could remember that"
- "I started by deciding to choose faces of people in my own race…"
- "… Plus he is African-American like me"

PixelPin

Upload a picture,

use 3 or more points as the “password”

random?

Images + Story

Invent a story for an image
or a sequence of images

"We went for a walk
in the park yesterday"

Fish-woman-girl-corn




Need to remember the order!

User Experiences

- 50% unable to invent a story, so try to pick four pleasing pictures and memorize their order
  - "I had no problem remembering the four pictures, but I could not remember the original order"
  - "… on the third try I found a sequence that I could remember, fish-woman-girl-corn. I would screw up the fish and corn order 50% of the time, but I knew they were the pictures"
- Picture selection biases
  - Males select nature and sports more than females
  - Females select food images more often

Shoulder Surfing

- Graphical password schemes are perceived to be more vulnerable to "shoulder surfing"
- Experimental study with graduate students at the University of Maryland Baltimore County
  - 4 types of passwords: Passfaces with mouse, Passfaces with keyboard, dictionary text password, non-dictionary text password (random words and numbers)
- Result: non-dictionary text password most vulnerable to shoulder surfing
  - Why do you think this is the case?

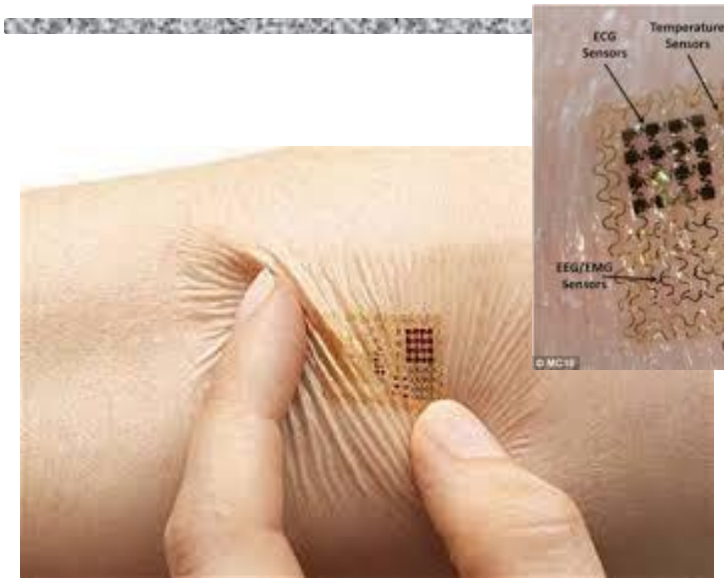
PetitionAgainstPasswords.com

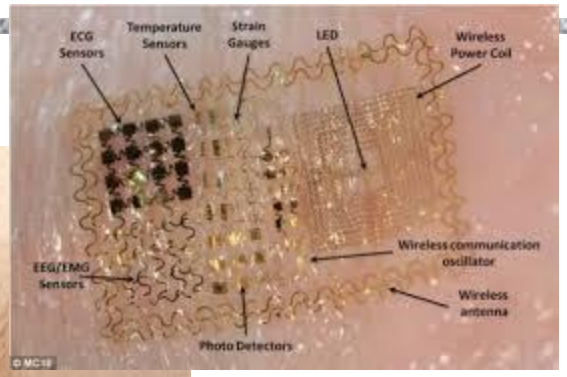
Alternatives to Passwords

Mobile phones, USB devices, special tokens, etc. etc.

LaunchKey

Alternatives from Motorola





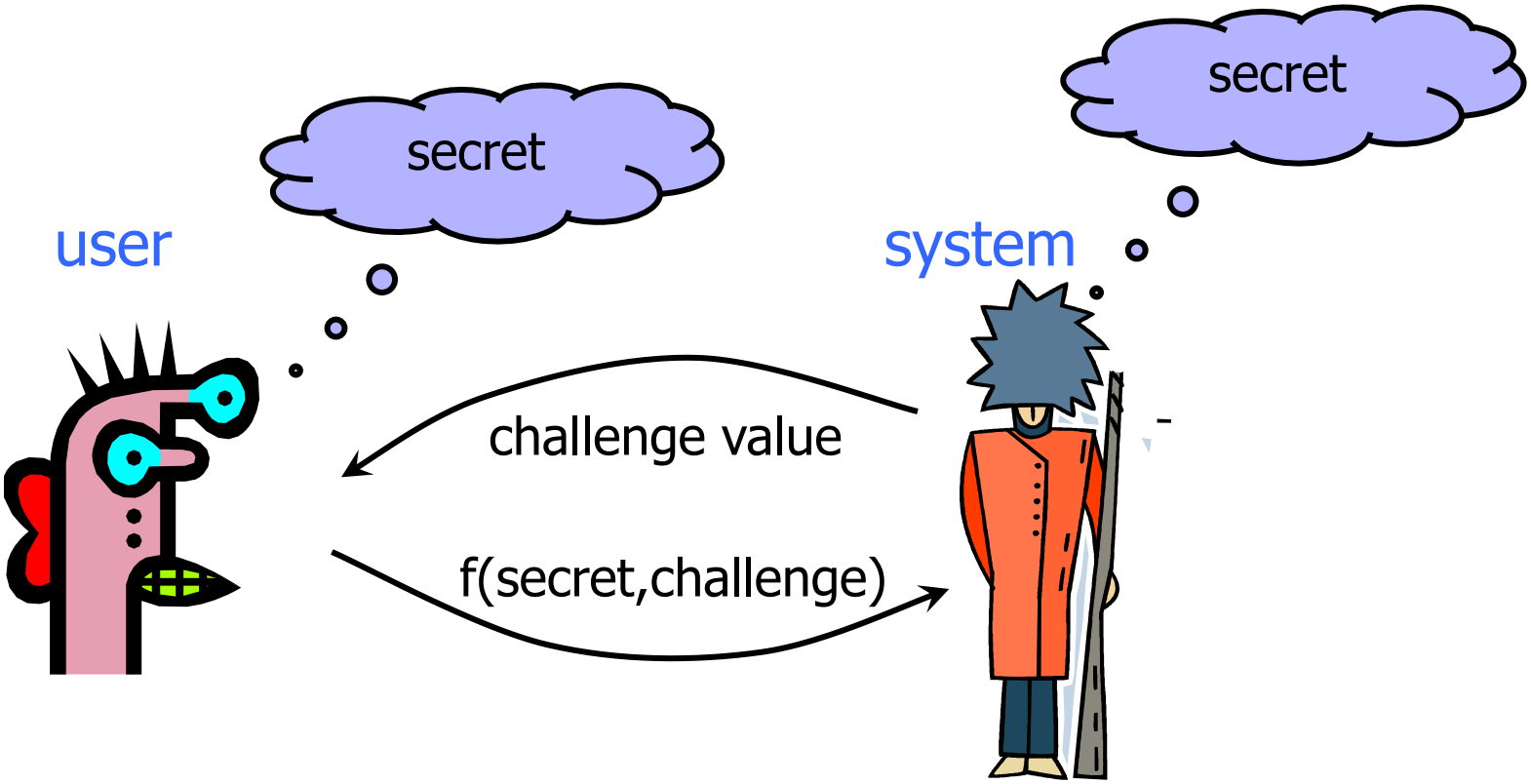
"… you can be sure that they'll be far more interested in wearing an electronic tattoo, if only to piss off their parents"

"The pill features a small chip with one switch that uses your stomach acids to activate an 18-bit ECG-like signal inside your body"

One-Time Passwords

- Idea: use a shared secret to derive a one-time password
- If the attacker eavesdrops on the network, he'll learn this password but it will be useless for future logins

Challenge-Response

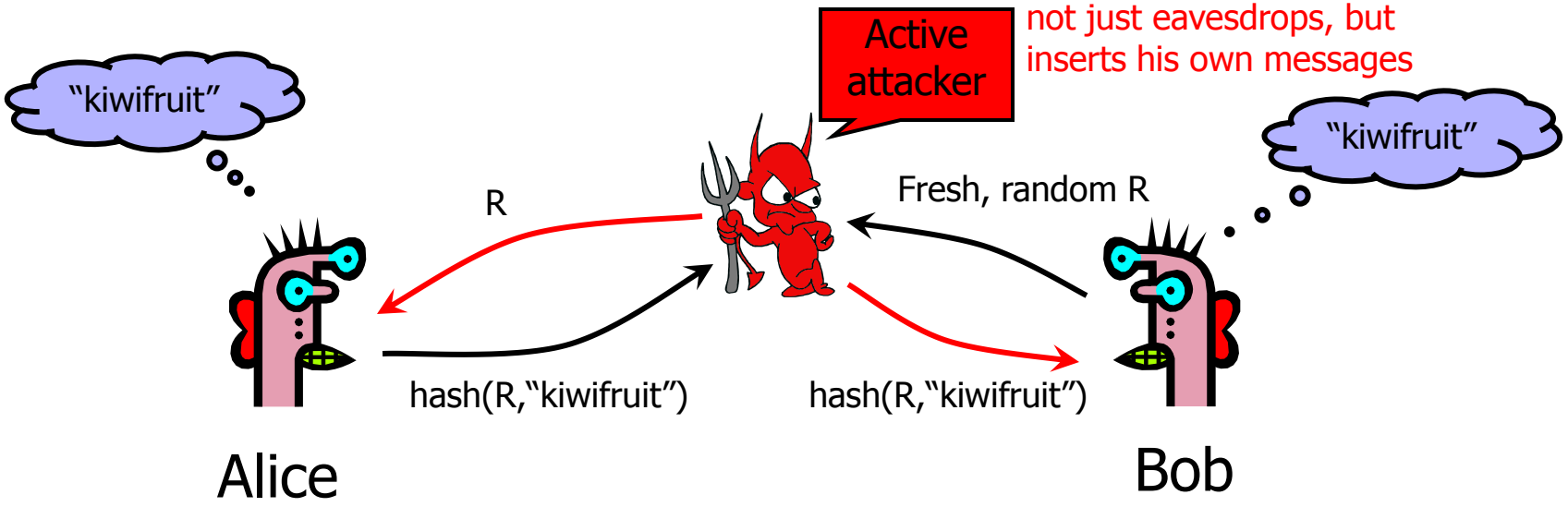


Why is this better than the password over a network?

Challenge-Response Authentication

- User and system share a secret (key or password)
- Challenge: system presents user with some string
- Response: user computes the response based on the secret and the challenge
  - Secrecy: difficult to recover secret from response
    - Cryptographic hashing or symmetric encryption work well
  - Freshness: if the challenge is fresh, attacker on the network cannot replay an old response
    - Fresh random number, counter, timestamp….
- Good for systems with pre-installed secret keys
  - Car keys; military friend-or-foe identification

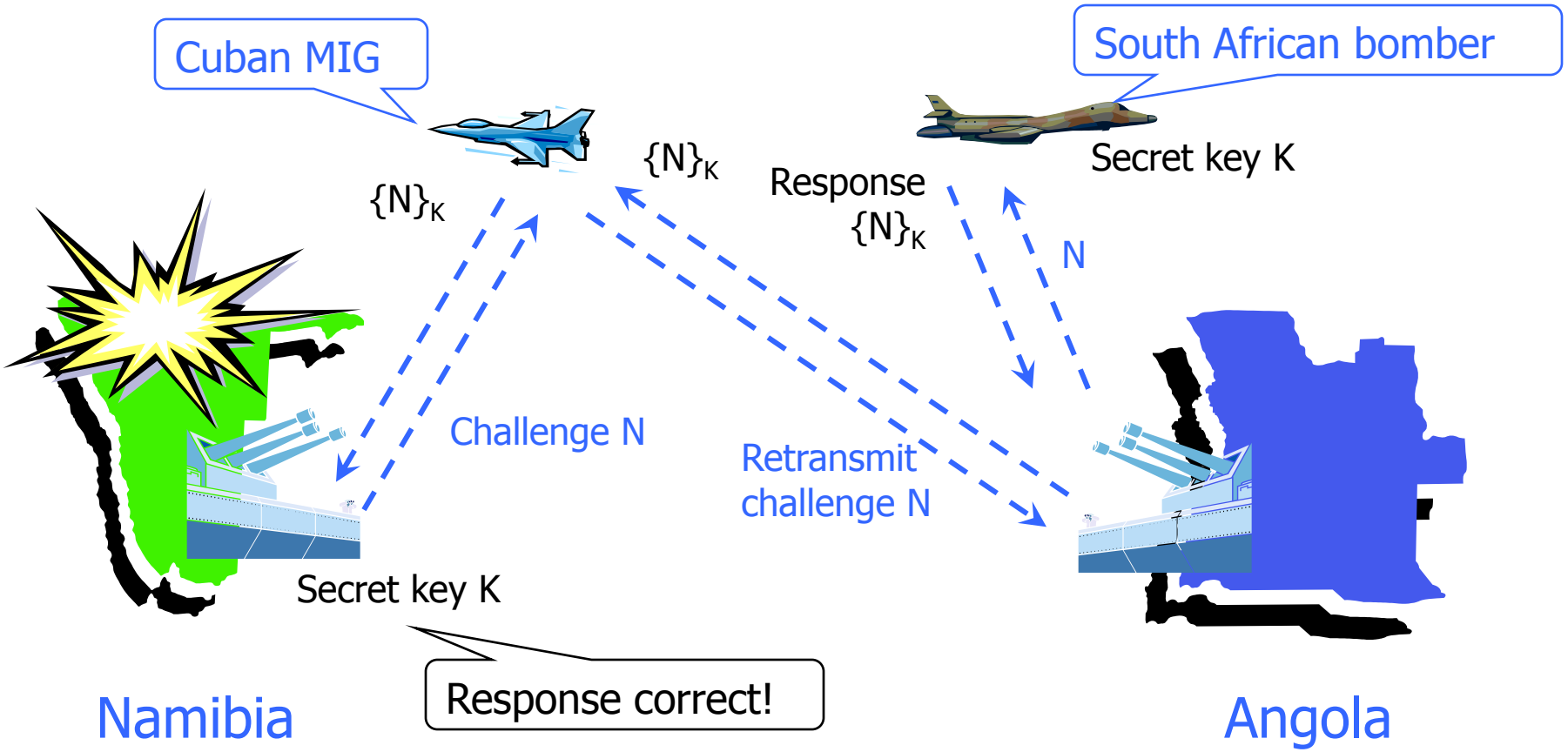
Man-in-the-Middle Attack



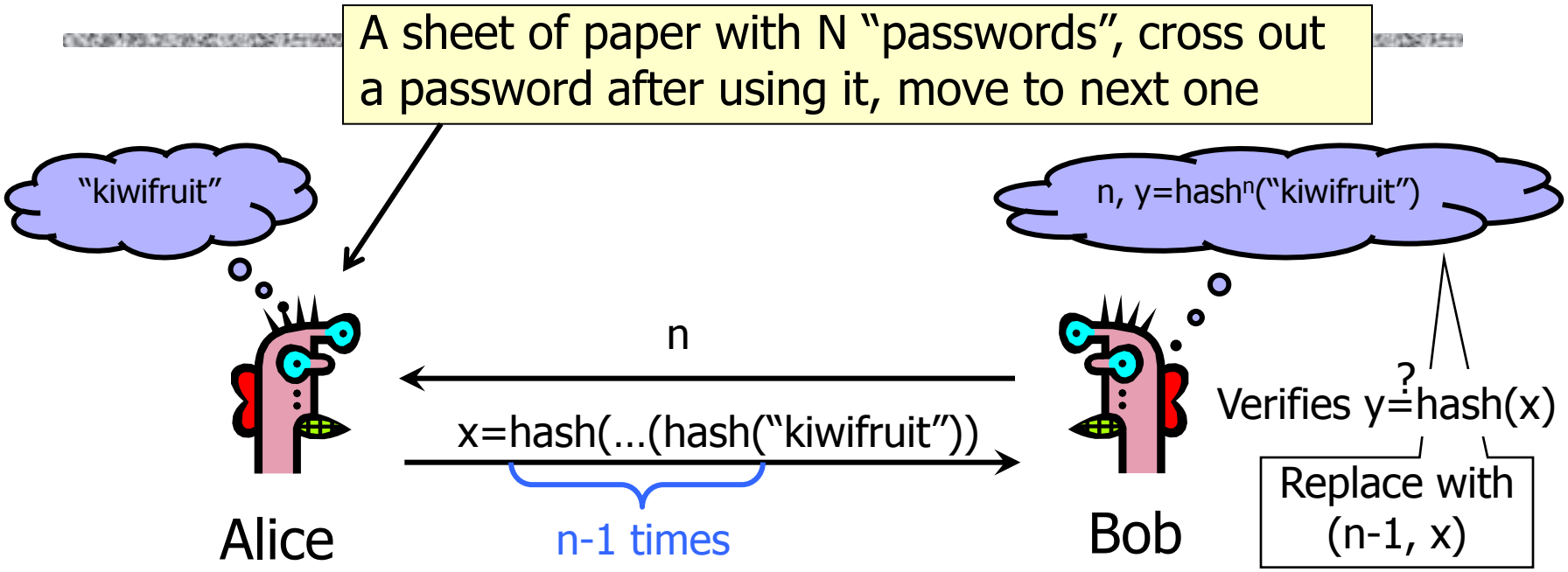
- Man-in-the-middle attack on challenge-response
  - Attacker successfully "authenticates" as Alice by simple replay
- This is an online attack
  - Attacker does not learn the shared secret
  - Attacker cannot "authenticate" as Alice when she is offline

MIG-in-the-Middle

[Ross Anderson]

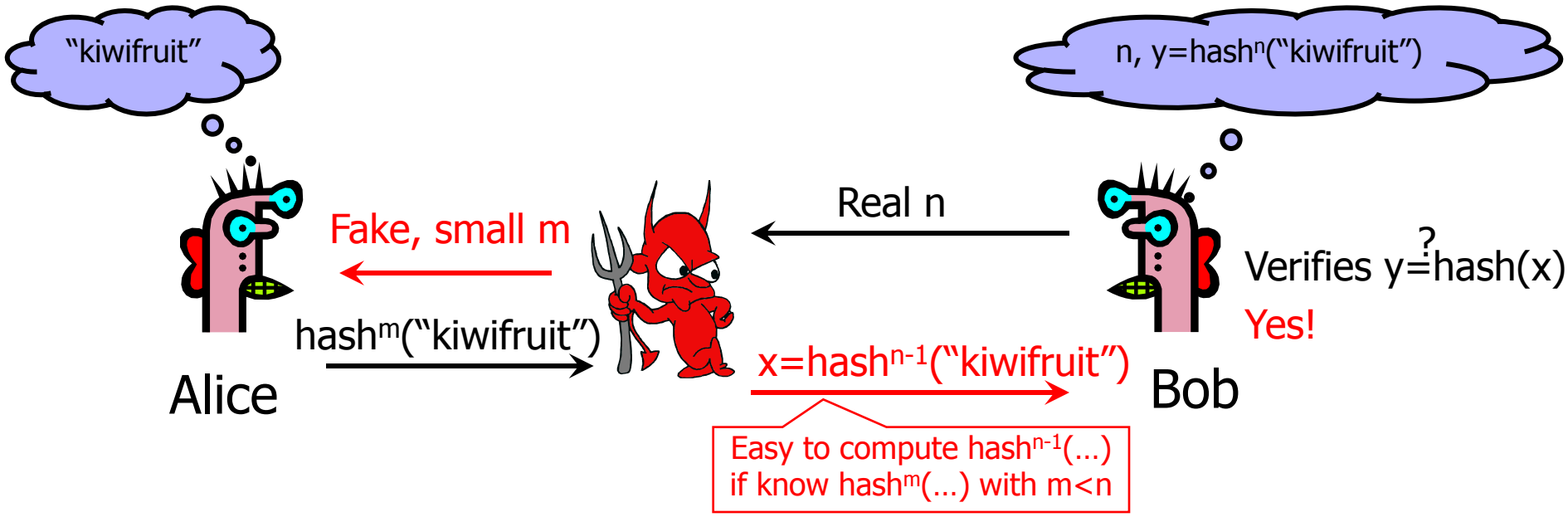


Lamport's Hash / S-Key



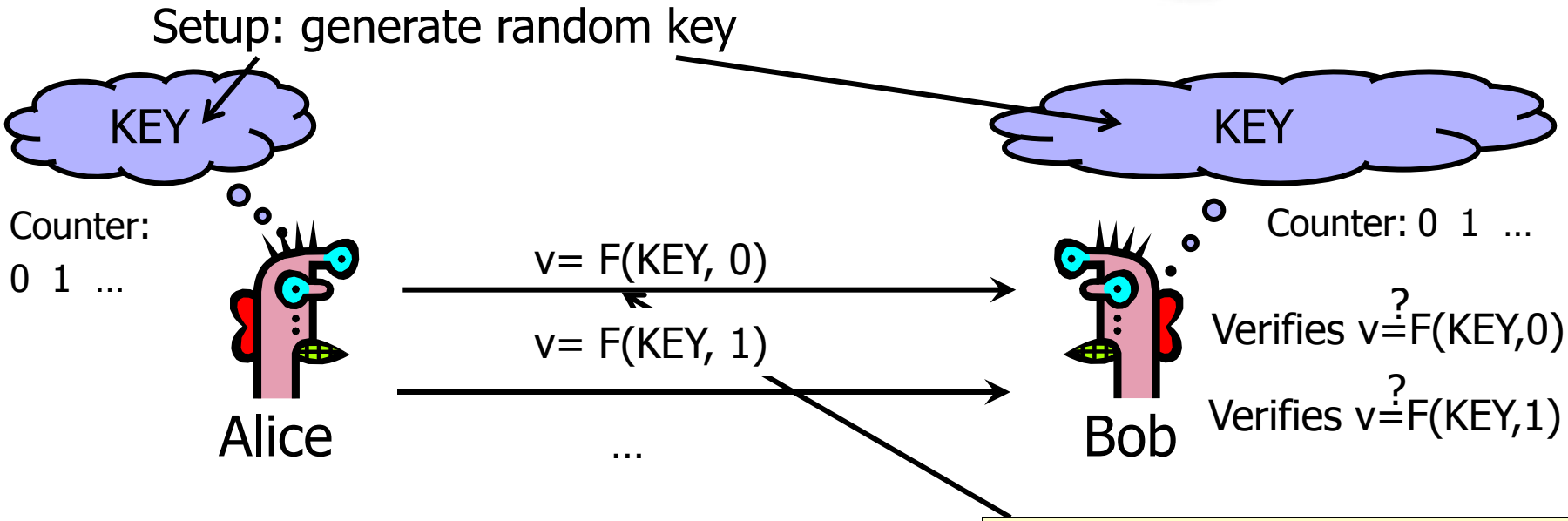
- Main idea: "hash stalk"
  - Moving up the stalk (computing the next hash) is easy, moving down the stalk (inverting the hash) is hard
  - n should be large - a stalk is only good for n authentications
- Verifier only needs the current tip of the stalk

"Small n" Attack



- First message from Bob is not authenticated!
- Alice should remember the current value of n

SecurID



- Advancing the counter
  - Time-based (60 seconds) or every button press
- Allow for skew in the counter value
  - 5-minute clock skew by default

RSA uses a custom function
Input: 64-bit key, 24-bit ctr
Output: 6-digit value