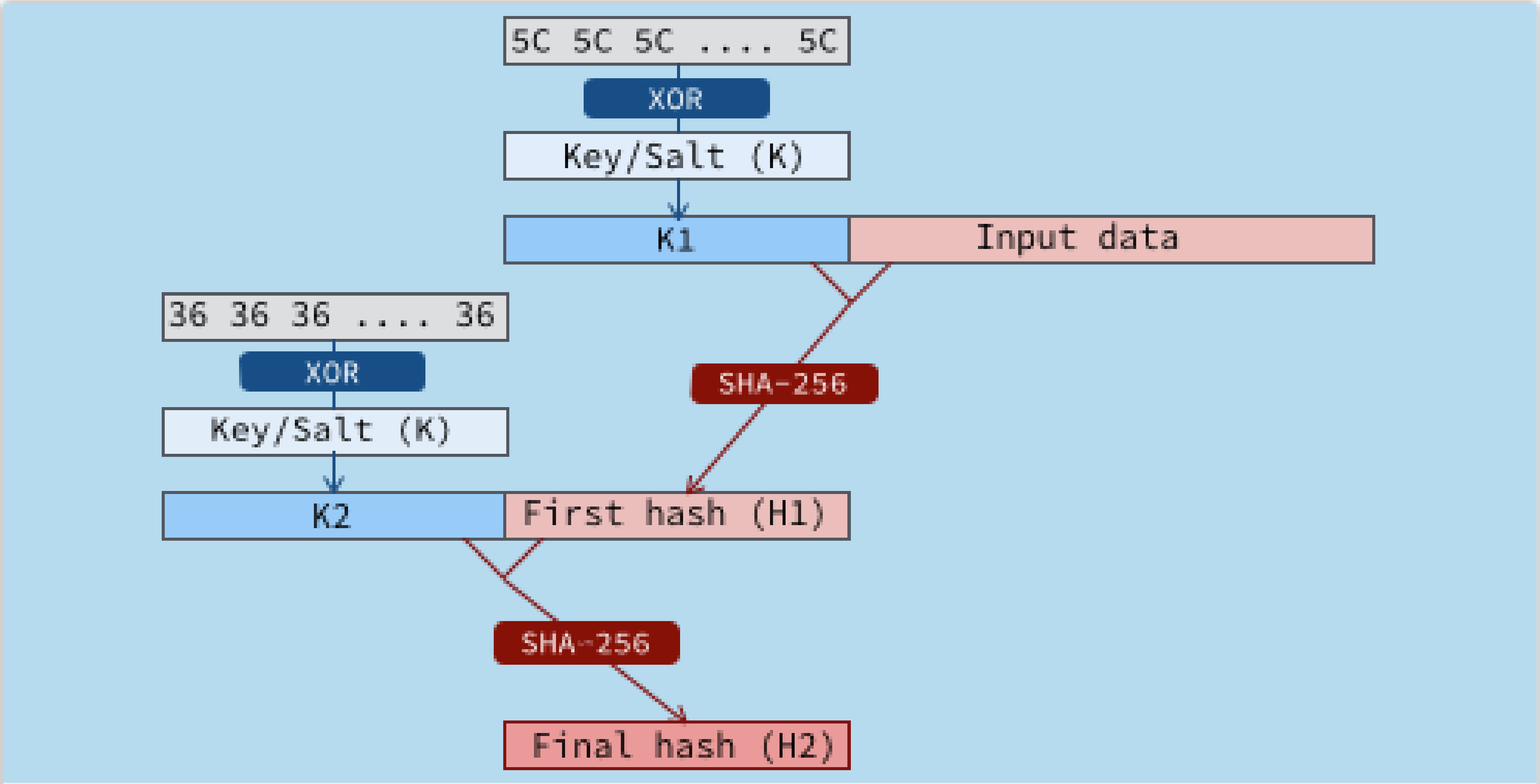
# HMAC

- Concatenation of keys with data can lead to some exploitable cryptographic scenarios
  - Outside the scope of this course

- HMAC (Keyed Hashed Message Authentication Code) allows us to combine the salt with the hash of the password in a more secure way

# HMAC with SHA



HMAC performs two iterations of a chosen cryptographic hash to create a "keyed hash"

Image source: https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/

# One more thing

- Our steps so far allow us the following guarantees:
  - User’s passwords should not be recoverable from a database
  - Identical/Similar passwords will have different hashes
  - The database does not “leak” the length of a user’s password

- The only problem remaining is that offline attackers, if they are dedicated enough, they can still brute-force their way into users with weak passwords

# 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

# Password Hash Cracking

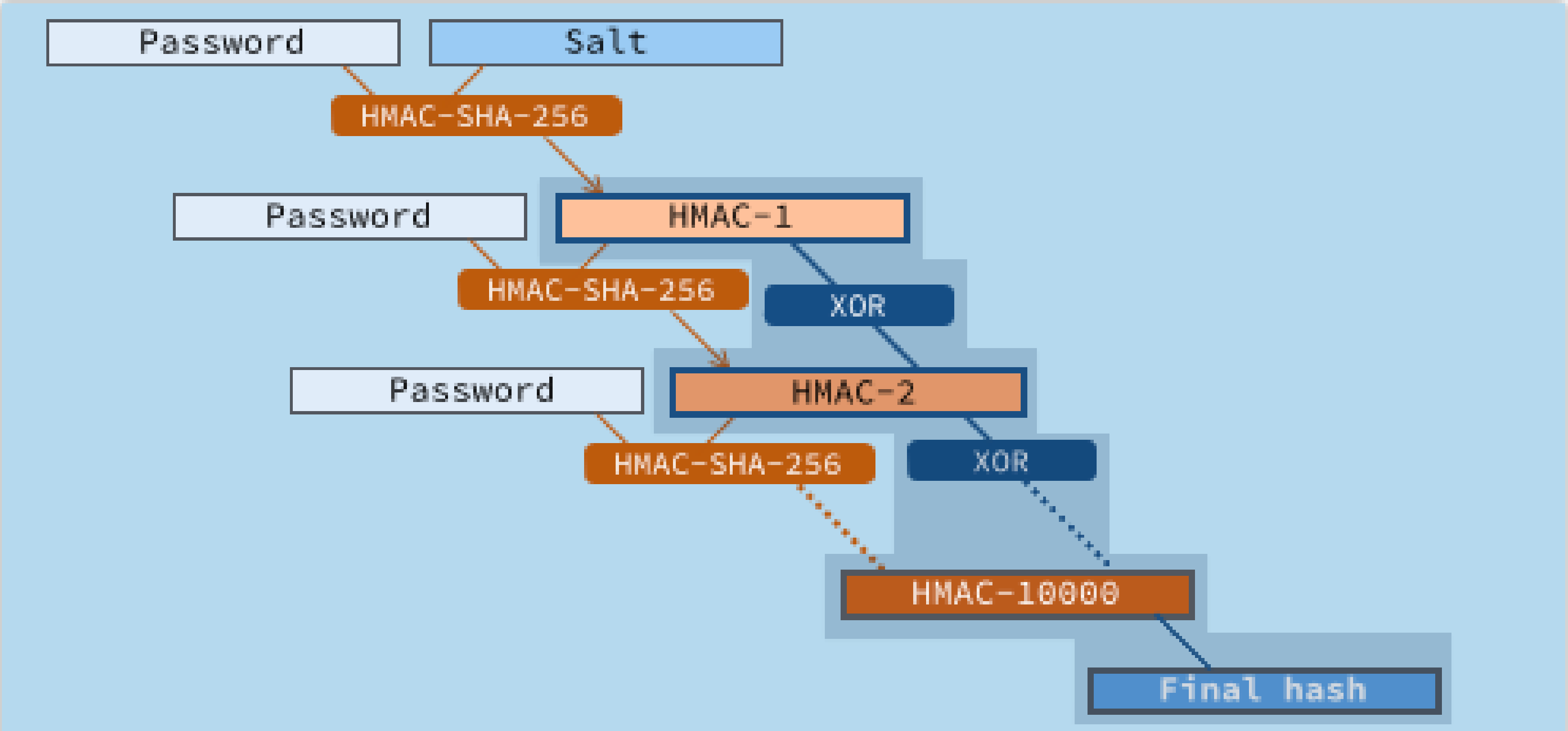
https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/

- 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
  - Project Mars, Crackq, etc.
  - Password-cracking as a service

# Hash stretching

- Why restrict ourselves to only one hash operation?
- If we perform multiple hashing rounds:
  - An attacker would need significantly more resources per cracking attempt
  - A server can still cope with the increased load because users are not authenticating all at the same time
- Standardized multi-round hashing algorithms
  - PBKDF2, brypt, scrypt

# PBKDF2 + HMAC-SHA-256



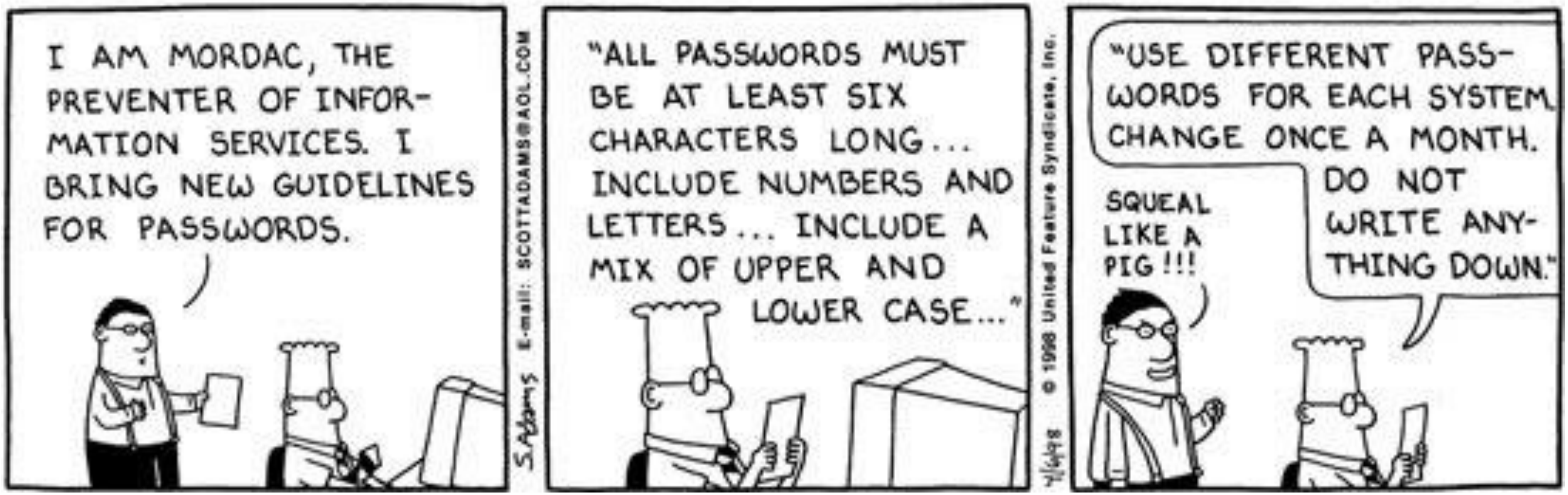
PBKDF2 using XOR to combine 10,000 successive HMAC-SHA-256 outputs into a final hash

Image source: https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/

# Back to users – 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

# Password Usability


I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES. I BRING NEW GUIDELINES FOR PASSWORDS.
"ALL PASSWORDS MUST BE AT LEAST SIX CHARACTERS LONG... INCLUDE NUMBERS AND LETTERS... INCLUDE A MIX OF UPPER AND LOWER CASE..."
"USE DIFFERENT PASSWORDS FOR EACH SYSTEM. CHANGE ONCE A MONTH. DO NOT WRITE ANYTHING DOWN."
SQUEAL LIKE A PIG!!!
S.Adams
E-mail: SCOTTADAMS@AOL.COM
© 1998 United Feature Syndicate, Inc.

# Password memorability

- Typically, **strength** of a password and **memorability** are working against each other
  - You can likely remember “jack123” better than “399%(mJjaweee”
- Various attempts have been made to come up with clever schemes for strong memorable passwords
  - “Abandon hope all ye who enter here” =>
  - aHaYwEh =>
  - aHaYvv3h

# How People Use Passwords

- Write them down
  - Password managers attempt to make this okay
- 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

# Password Managers

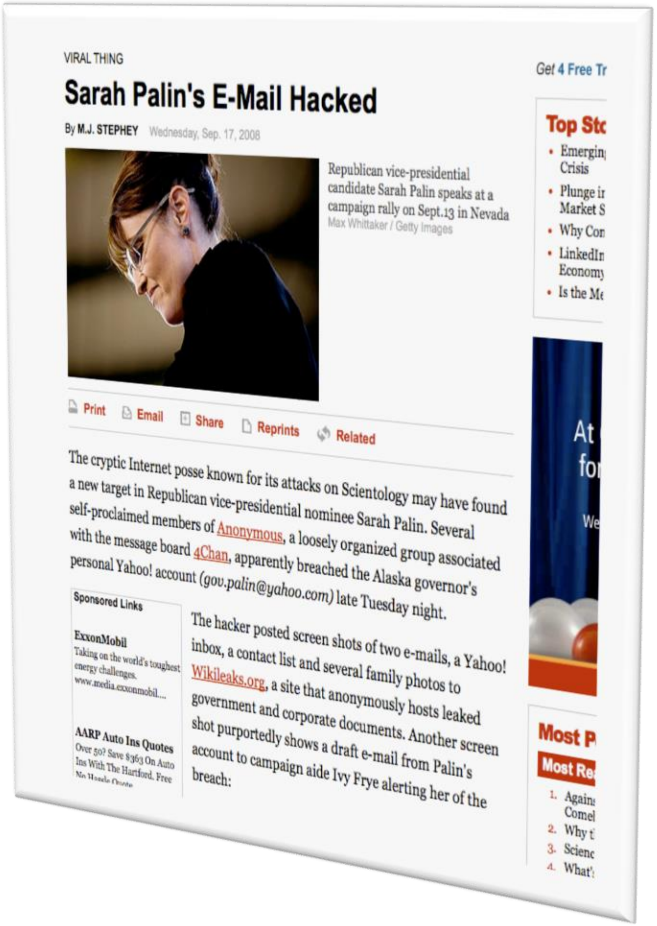
- One place where all your passwords are stored
  - This place is protected with one master password
  - Flavors:
    - Online versus Offline (e.g. LastPass versus KeePass)

- Benefits
  - No need to remember any more passwords (other than the master phrase)
  - Unique password per website (no more password reuse)
  - Most password managers also have their own password generators to automatically create strong passwords
- Disadvantages
  - Single-point of failure
    - This can be easily mitigated by storing multiple copies of the database
  - Lock yourself out
    - If you forget your master password, there is no way to recover passwords
  - Cannot authenticate to services if you don't have access to the password manager

# 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

Get 4 Free Tr

**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

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:

Top Sto
- Emergin Crisis
- Plunge ir Market S
- Why Con
- LinkedIn Economy
- Is the Me

At
fo
We

Most P
Most Re
1. Again Comel
2. Why t
3. Scienc
4. What'

# 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

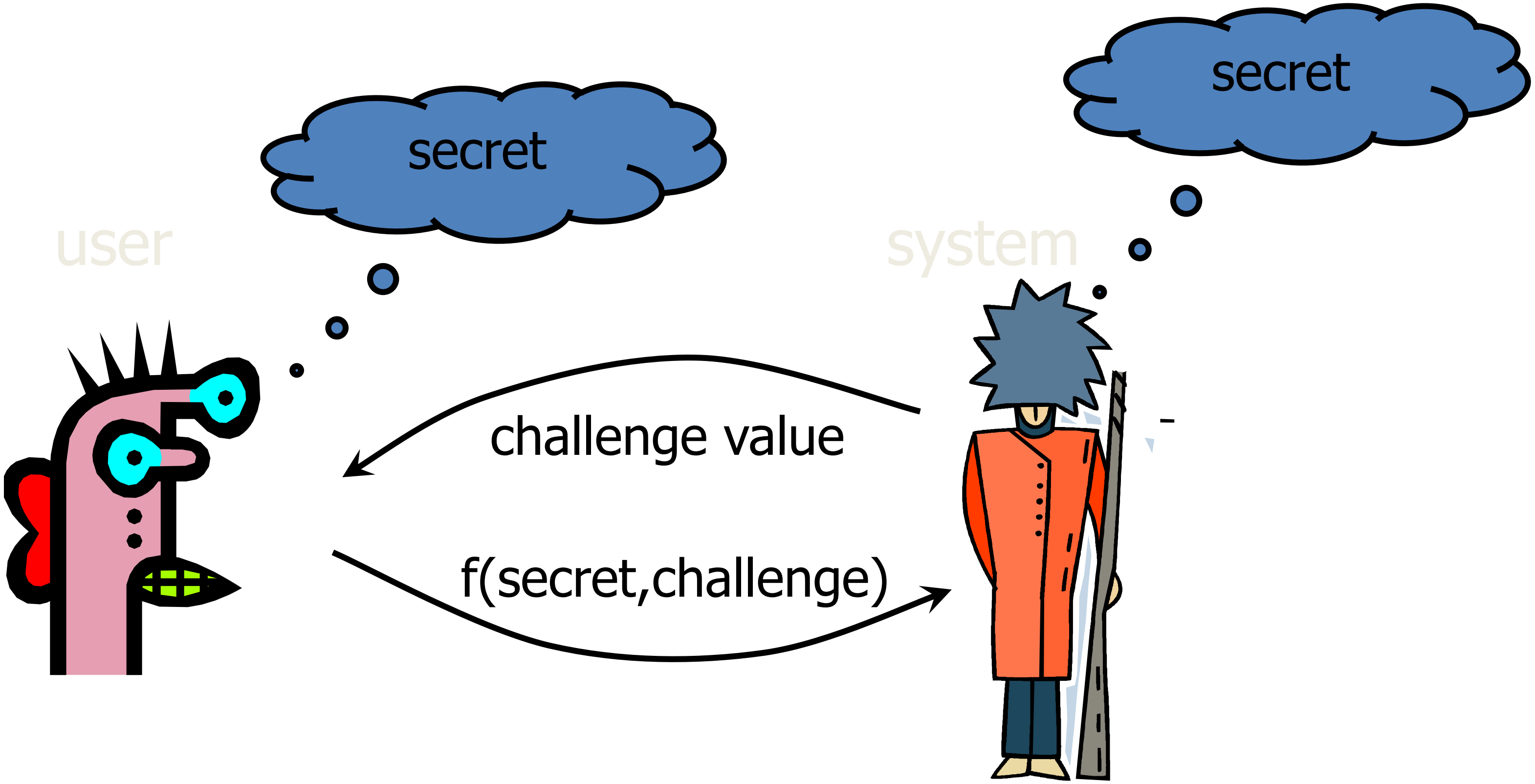
# …or Easy to Forget

- 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

# Replay attacks and possible solutions

- The standard, password-based authentication is vulnerable to **replay attacks**
  - A network attacker can see the password in traffic, and then later reuse to authenticate as the victim
- We can encrypt the entire channel to protect against this (explore this later in class) but we can also tackle it with **one-time passwords (OTP)**

# Challenge-Response

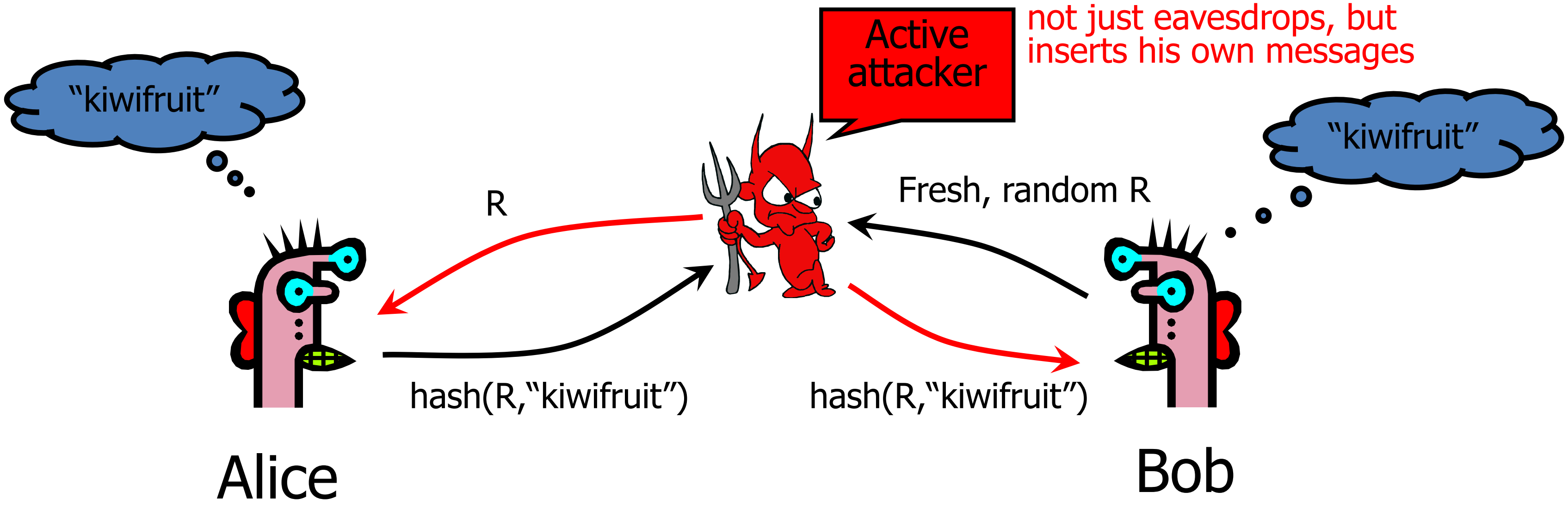


Why is this better than the password over a network?

# 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

# Making passwords stronger

- Passwords belong to the “what you know” category…
- Using “what you have” to strengthen the overall security of a system

- When more than techniques are used for authentication, then we have multiple-factor authentication
  - E.g. 2 Factor Authentication: password + phone

# Something you have

- Things one can have
  - Access to your smartphone
    - Has gained a lot of traction recently due to popular web applications (Gmail, Twitter, etc.) supporting it
  - A bank card
  - A security token
    - A piece of hardware containing crypto that either generates one-time passwords or does a challenge-response protocol
  - A badge

- Problems
  - Stolen / forgotten / lost / duplicated
    - Higher cost to change than passwords
  - Cost of user education and support

# Something you have - SMS

- Text messages (SMS) as a 2-factor authentication method is falling out of favor.
  - NIST (National Institute of Standards and Technology) has mentioned that it is deprecated and when possible, services should use hardware tokens or smartphone apps to deliver codes
- Reasons
  - Too many incidents of attackers social engineering phone companies into sending them SIM cards because the real owner “lost their phone”
  - Telcos in authoritarian governments can cooperate with their governments
  - Phone networks and their protocols are not exactly the most secure ones
- Moral of the story
  - Use when possible something other than SMS for 2FA
  - SMS-based 2FA is still *MUCH* better than just password-based authentication