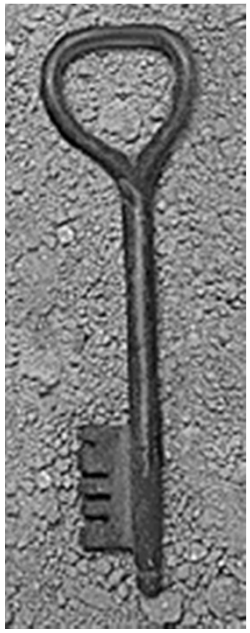
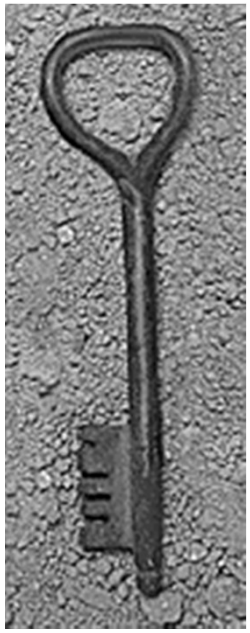
Authentication

the process of reliably verifying the identity of someone (or something)

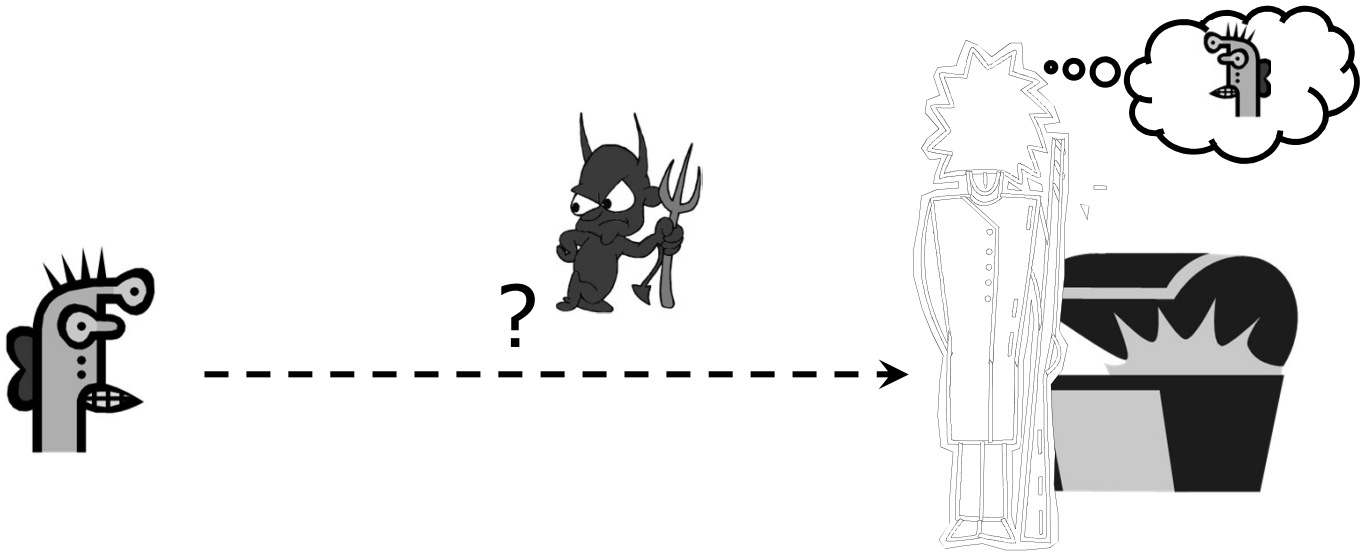


Agenda

- Basic Concepts
- Password-Based Authentication
- Biometrics
- Authentication Protocols
- Advanced Topic: Graphical Passwords

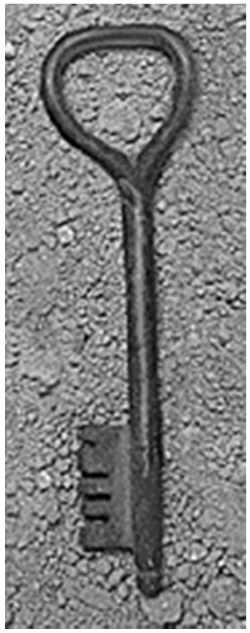


Basic Problem



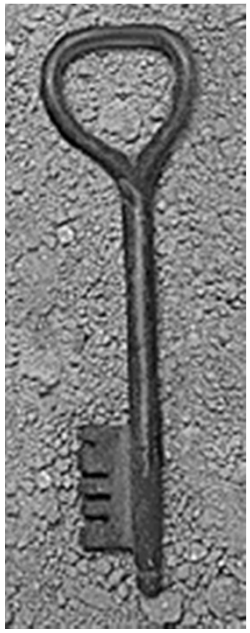
How do you prove to someone that
you are who you claim to be?

Any system with access control must solve this problem



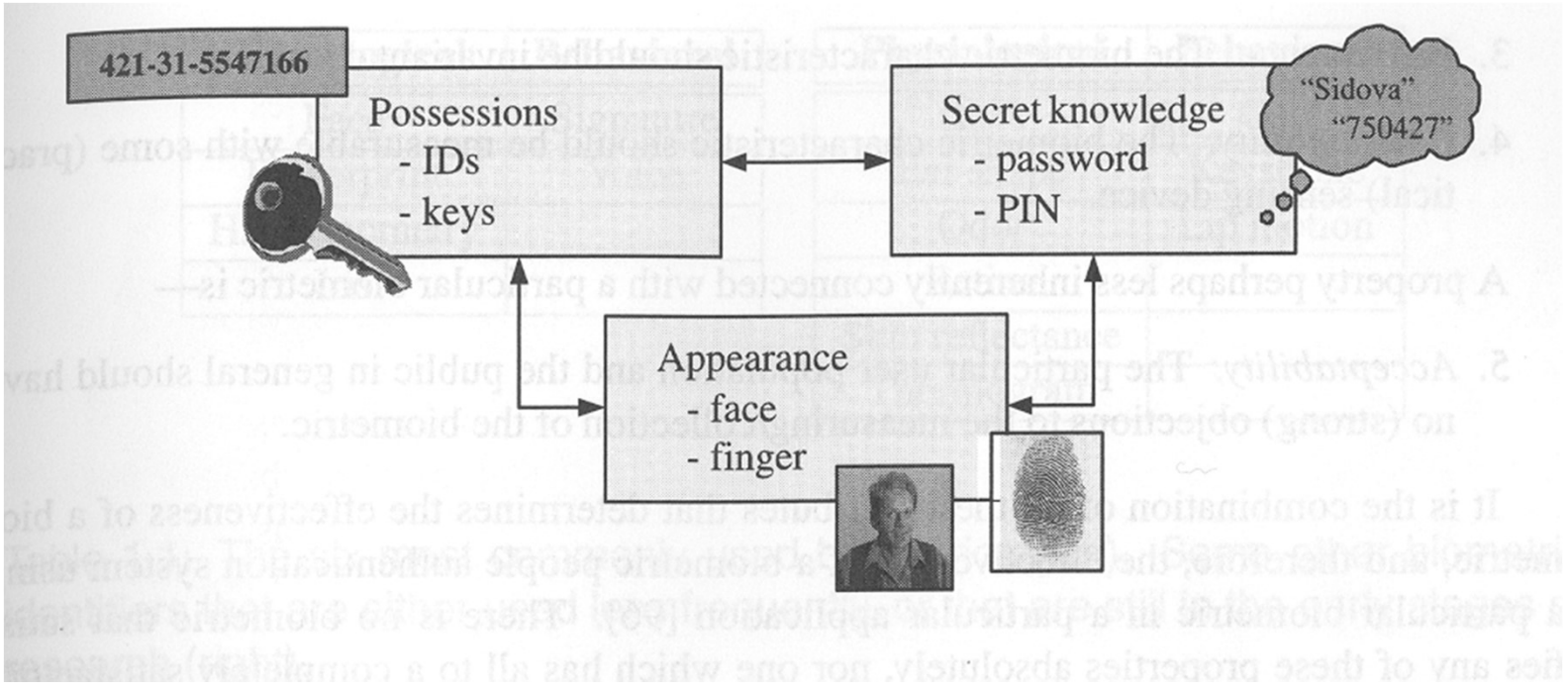
Many Ways to Prove Who You Are

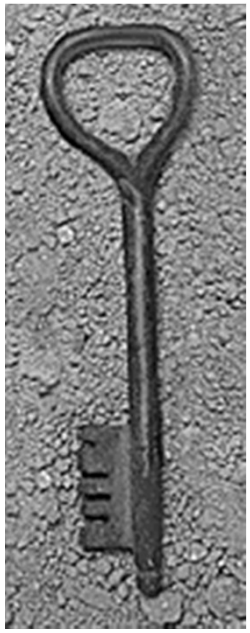
- What you know
  - Passwords
  - Secret key
- Where you are
  - IP address
- What you are
  - Physiological (fingerprints, face, iris, ...)
  - Behavioral (walking, keystroke pattern, talking, ...)
- What you have
  - Secure tokens



Authentication

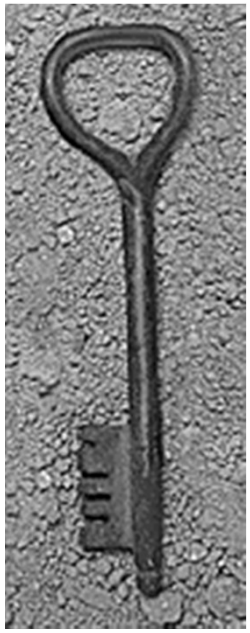
- Modes of authentication are sometimes combined
  - User id + password
  - ATM card + password
  - Passport + face picture and signature





Agenda

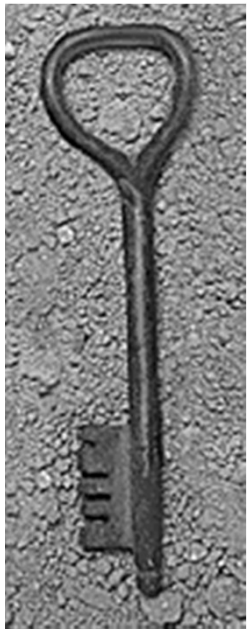
- Basic Concepts
- Password-Based Authentication
- Biometrics
- Authentication Protocols
- Advanced Topic: Graphical Passwords



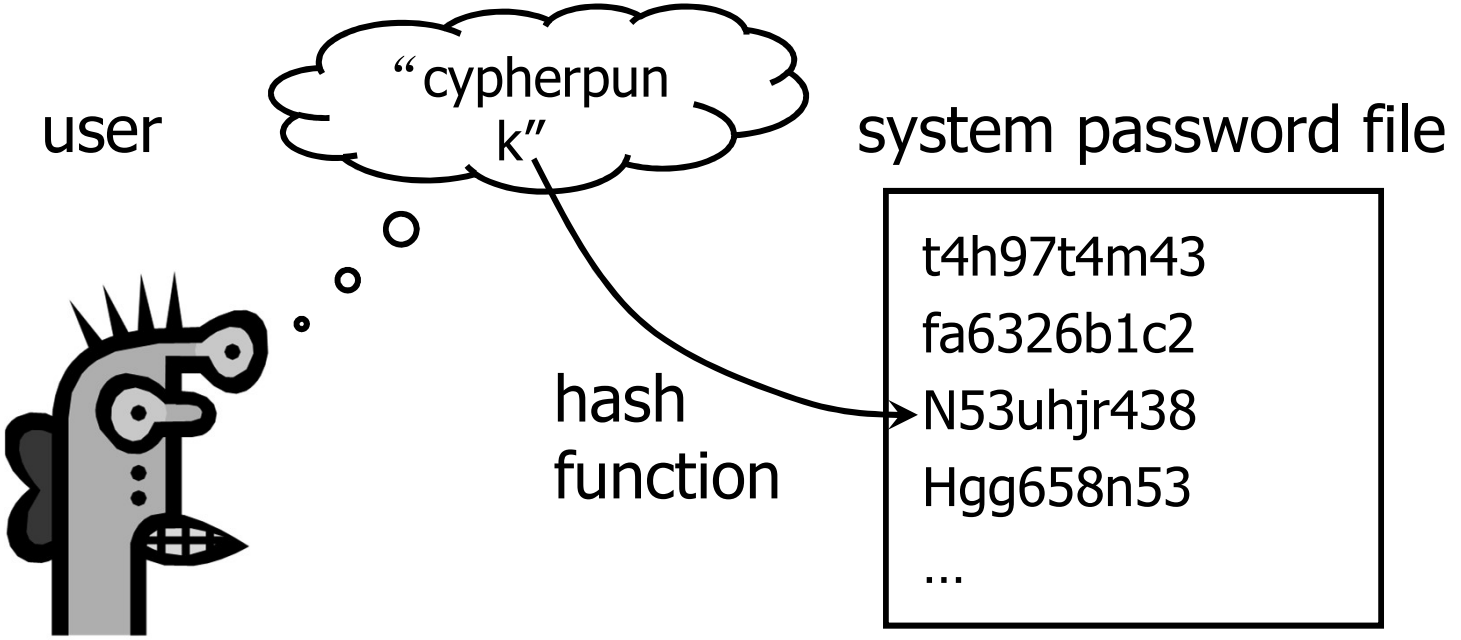
Password-Based Authentication

- User has a secret password.

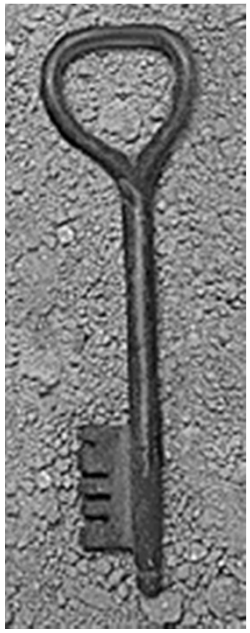
  System checks it to authenticate the user.
  - Vulnerable to eavesdropping when password is communicated from user to system
- How is the password stored?
  - Password file is difficult to keep secret
- How easy is it to guess the password?
  - Easy-to-remember passwords are easy to guess
- How does the system check the password?



UNIX-Style Passwords: Hashing

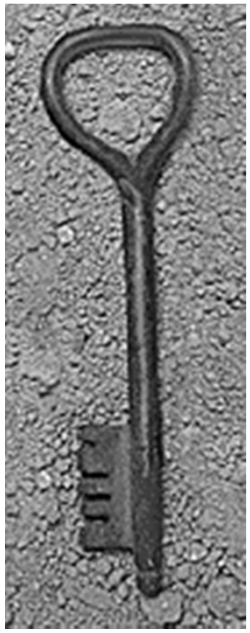


- Instead of user password, store H(password)
- When user enters password, compute its hash on the fly, and compare with entry in password file
  - System does not store actual passwords! Resolve the password file protection problem
- Hash function H must be One-way



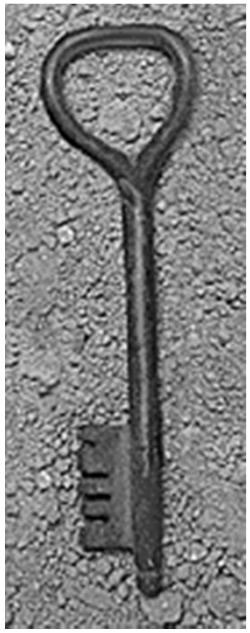
Traditional UNIX Password System

- Uses DES encryption as if it were a hash function
  - Encrypt NULL string using password as the key
    - Truncates passwords to 8 characters!
  - Artificial slowdown: run DES 25 times why?
- Problem: passwords are not truly random
  - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are $94^8 \approx 6$ quadrillion($1M^4$) possible 8-character passwords
  - Humans like to use dictionary words, human and pet names ≈ 1 million common passwords

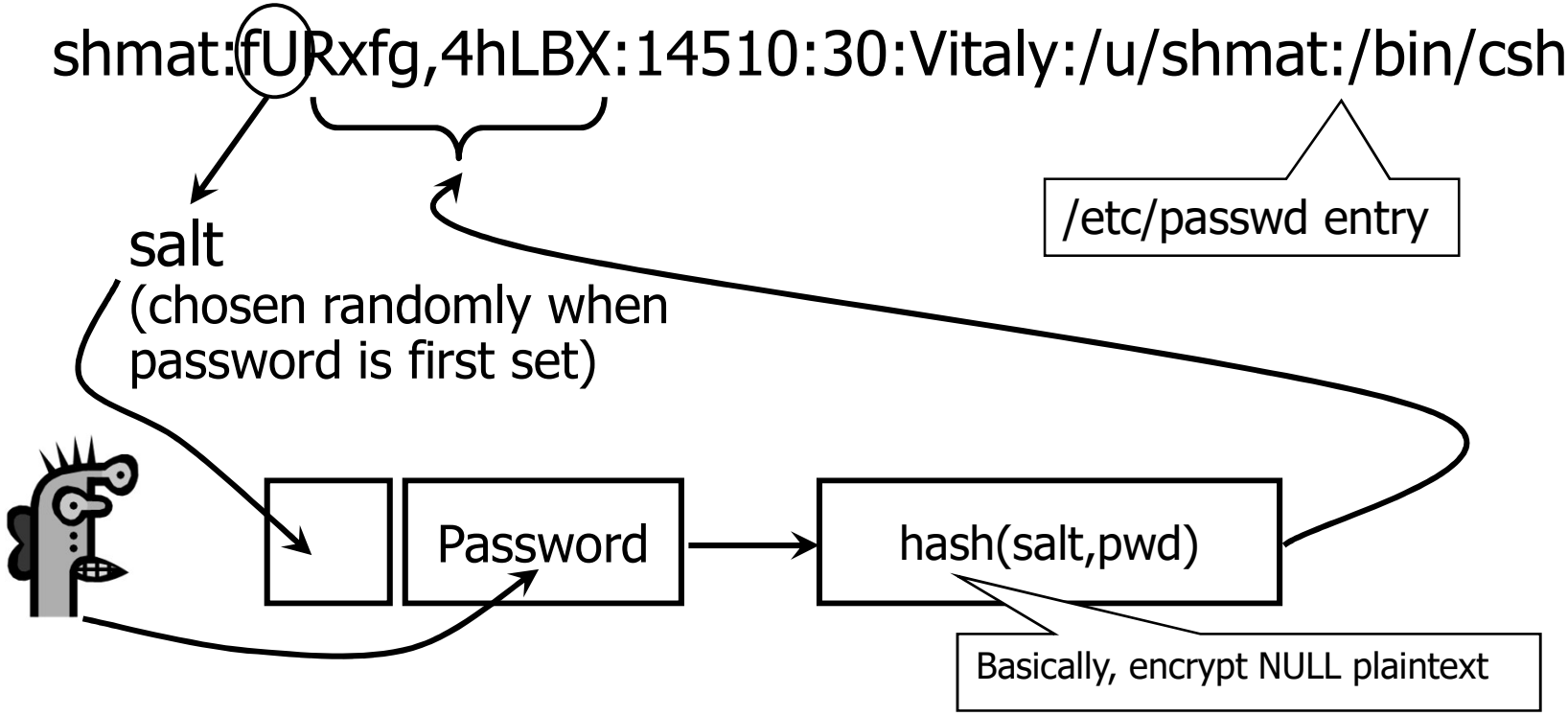


Traditional Dictionary Attack

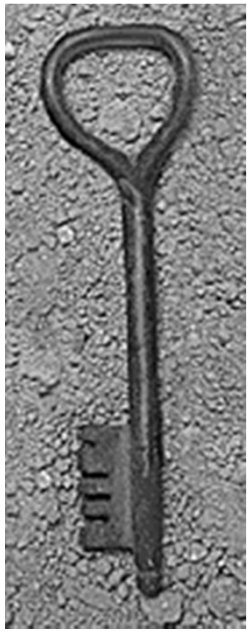
- Password file /etc/passwd is world-readable
  - Contains user IDs and group IDs which are used by many system programs
- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can compute H(word) for every word in the dictionary and see if the result is in the password file
  - With 1,000,000-word dictionary and assuming 10 guesses per second, brute-force online attack takes 50,000 seconds (14 hours) on average
    - This is very conservative. Offline attack is much faster!



Upgrading Phase 1: Salting

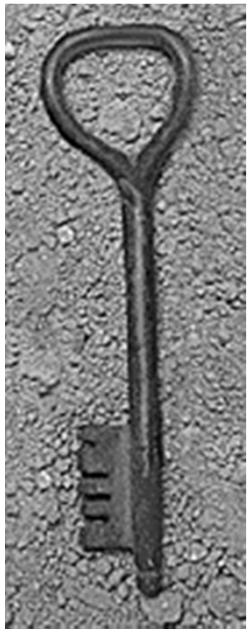


- Users with the same password have <u>different</u> entries in the password file
- Dictionary attack is still possible!



Advantages of Salting

- Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
  - Same hash function on all UNIX machines
  - Same passwords hash to same values; one table of hash values can be used for all password files
- With salt, attacker must compute hashes of all dictionary words once for each password entry
  - With 12-bit random salt, same password can hash to 2^{12} different hash values
  - Attacker must try all dictionary words for each salt value in the password file



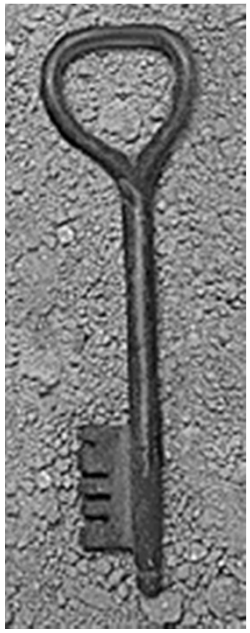
Upgrading Phase 2: Shadow Passwords

shmat:x:14510:30:Vitaly:/u/shmat:/bin/csh

/etc/passwd entry

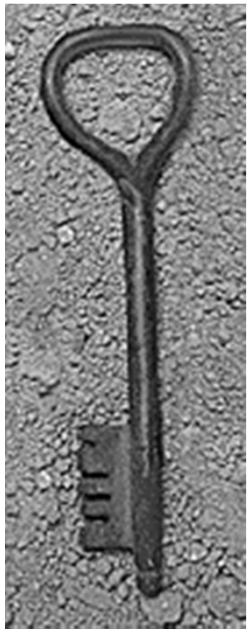
Hashed password is not
stored in a world-readable file

- Store hashed passwords in /etc/shadow file which is only readable by system administrator (root)
- Add expiration dates for passwords
- Early Shadow implementations on Linux called the login program which had a buffer overflow!



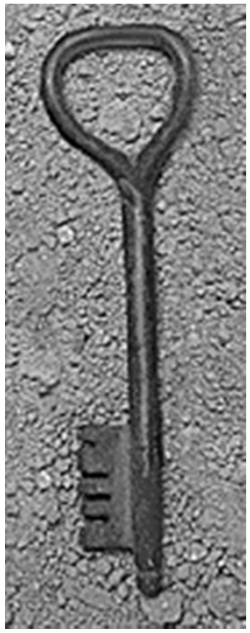
Other upgradings

- 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
- Rely on the difficulty of computer vision
  - Face recognition is easy for humans, hard for machines
  - Present user with a sequence of faces, he must pick the right face several times in a row to log in



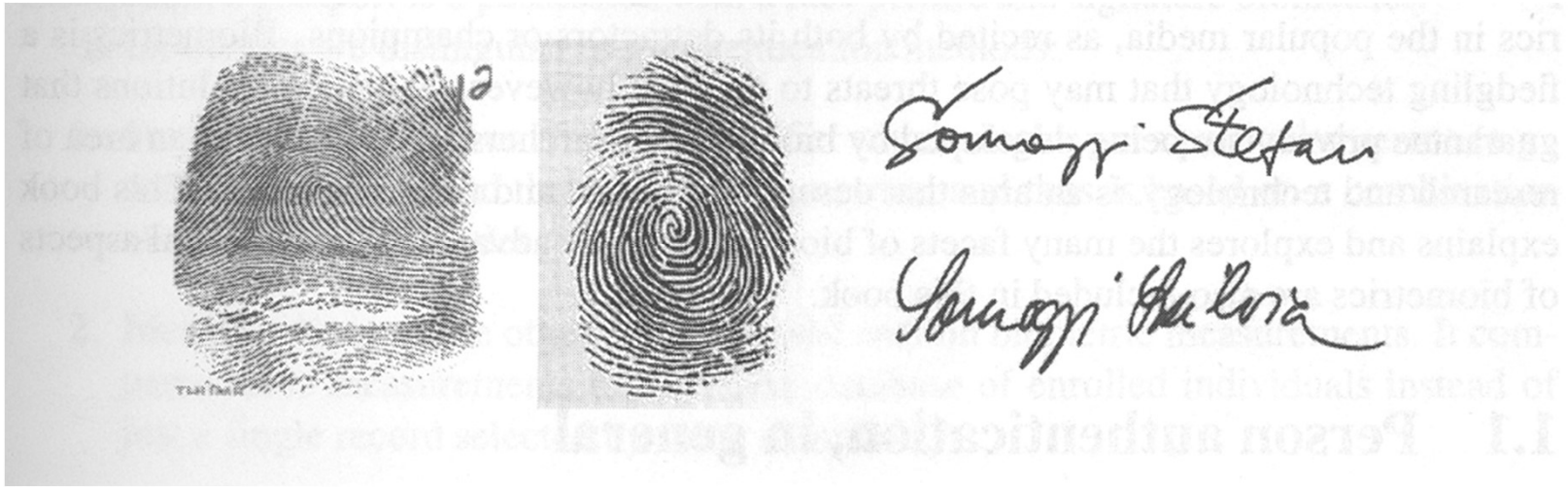
Agenda

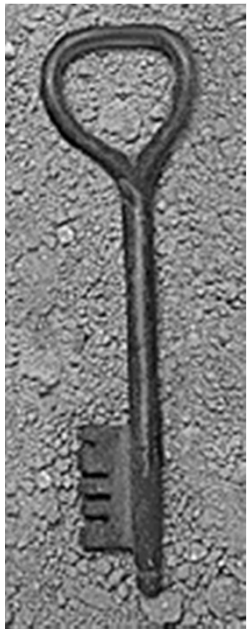
- Basic Concepts
- Password-Based Authentication
- Biometrics
- Authentication Protocols
- Advanced Topic: Graphical Passwords



What About Biometrics?

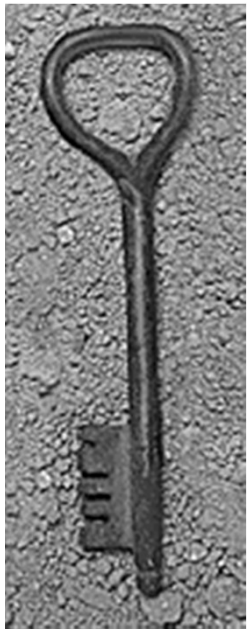
- Biometrics: Science of identifying, or verifying the identity of, a person based on physiological or behavioral characteristics.





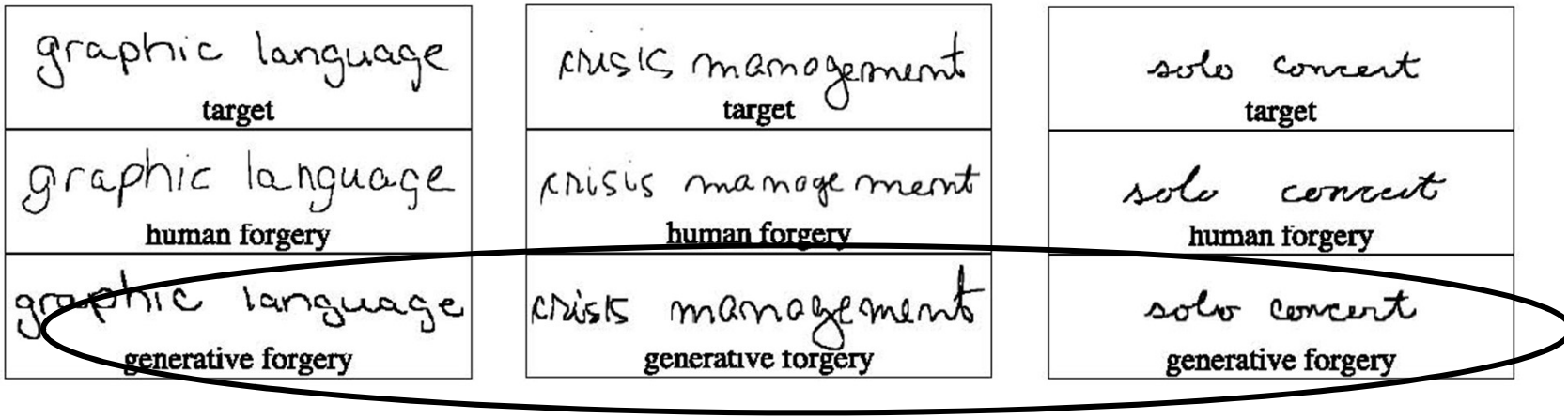
Biometrics

- Use a person's physical characteristics
  - fingerprint, voice, face, keyboard timing, …
- Advantages
  - Cannot be disclosed, lost, forgotten
- Disadvantages
  - Cost, installation, maintenance
  - Reliability of comparison algorithms
    - Fraud False: Allow access to unauthorized person
    - Insult False: Disallow access to authorized person
  - Privacy?
  - If forged, how do you revoke?

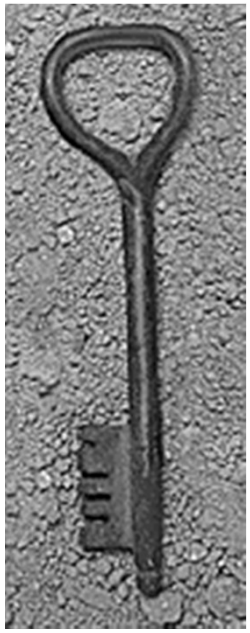


Authentication by Handwriting

[Ballard, Monrose, Lopresti]

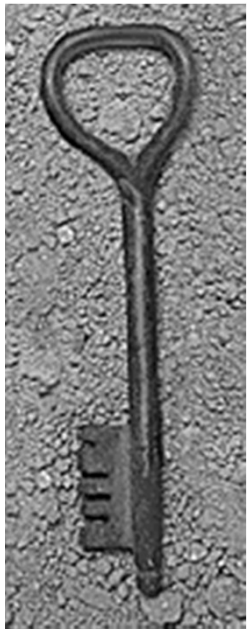


Generated by computer algorithm trained on handwriting samples



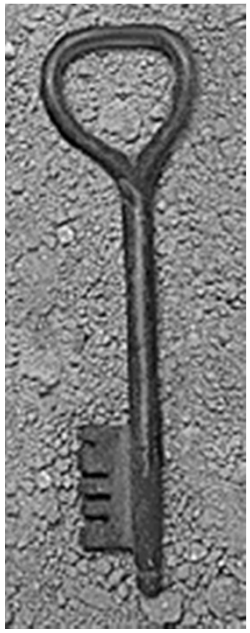
Biometric Error Rates

- "Fraud rate" vs. "insult rate"
  - Fraud = system accepts a forgery (false accept)
  - Insult = system rejects valid user (false reject)
- Increasing acceptance threshold increases fraud rate, decreases insult rate
  - Usually, Fraud rate * Insult rate is almost a constant
  - Pick a threshold depending the usage

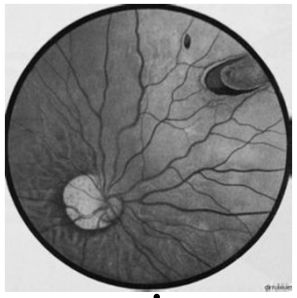


Other Biometrics (1)

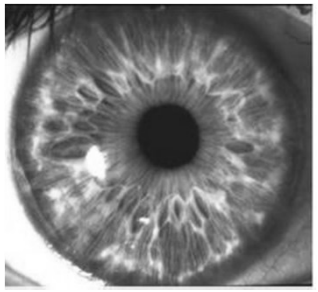
- Face recognition (by a computer algorithm)
  - Error rates up to 20%, given reasonable variations in lighting, viewpoint and expression
- Fingerprints
  - Traditional method for identification
  - 1911: first US conviction on fingerprint evidence
  - U.K. traditionally requires 16-point match
    - Fraud rate < 0.001%, Insult rate < 0.1%
  - Fingerprint damage impairs recognition



Other Biometrics (2)

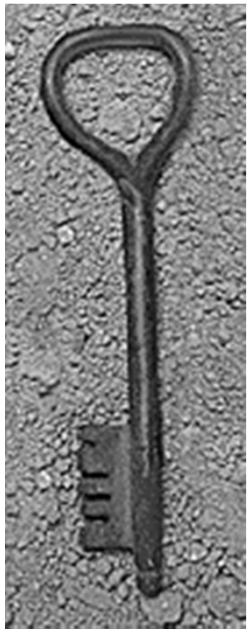


retina



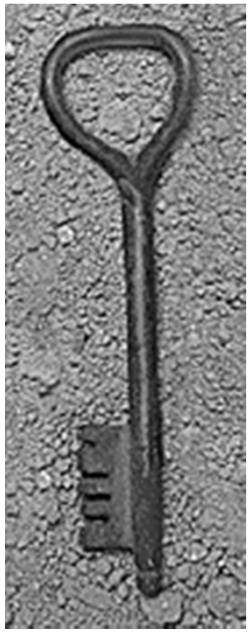
Iris

- Iris scanning
  - Irises are very random, but stable through life
    - Different between the two eyes of the same individual
  - 256-byte iris code based on concentric rings between the pupil and the outside of the iris
  - Equal error rate better than < 0.0001%
  - Best biometric mechanism currently known
- Hand geometry
  - Used in nuclear premises entry control, INSPASS (discontinued in 2002)
- Voice, ear shape, vein pattern, face temperature



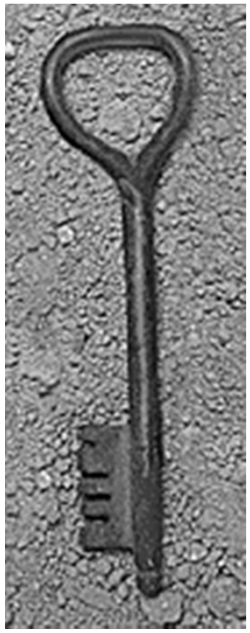
Risks of Biometrics

- Criminal gives an inexperienced policeman fingerprints in the wrong order
  - Record not found; gets off as a first-time offender
- Can be attacked using recordings
  - Ross Anderson: in countries where fingerprints are used to pay pensions, there are persistent tales of "Granny's finger in the pickle jar" being the most valuable property she bequeathed to her family



Agenda

- Basic Concepts
- Password-Based Authentication
- Biometrics
- Authentication Protocols
- Advanced Topic: Graphical Passwords

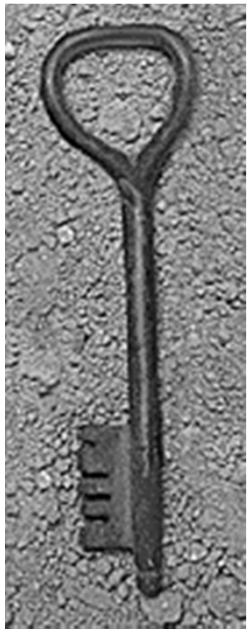


Challenge-response Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"

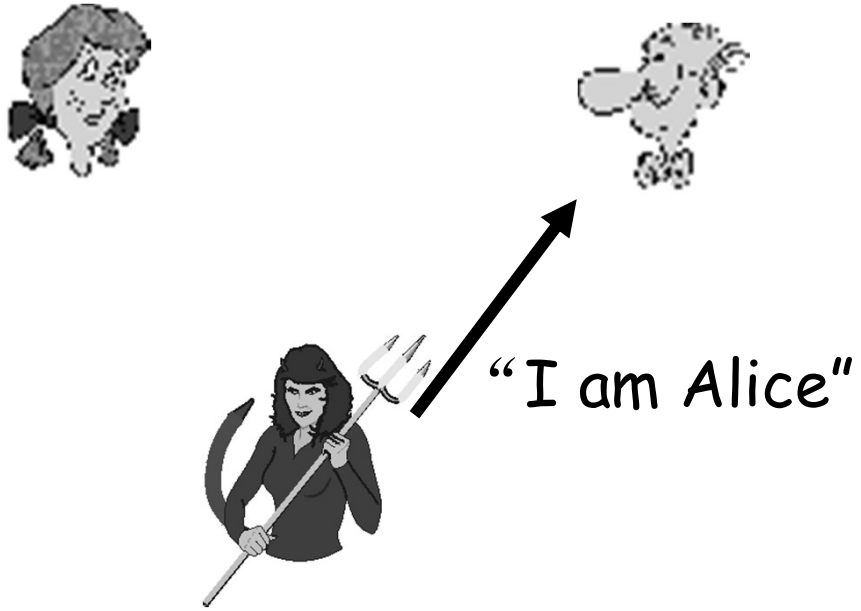
Failure scenario??



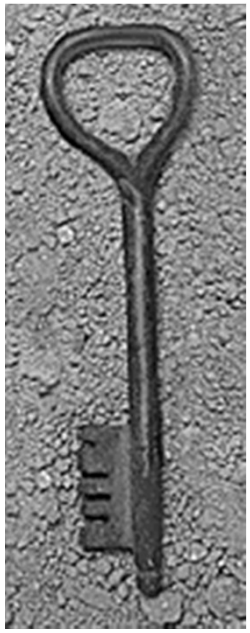
Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"

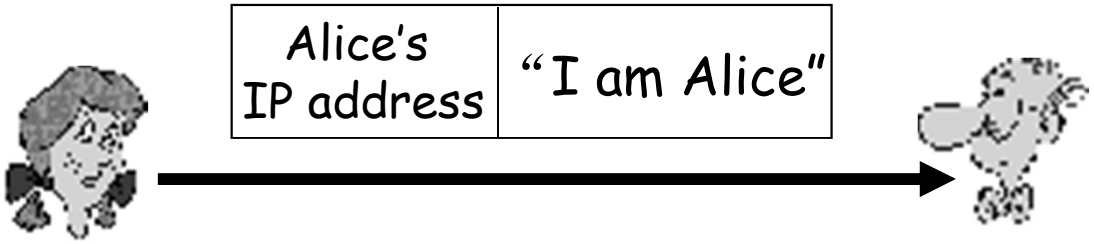


in a network,
Bob can not "see"
Alice, so Trudy simply
declares
herself to be Alice

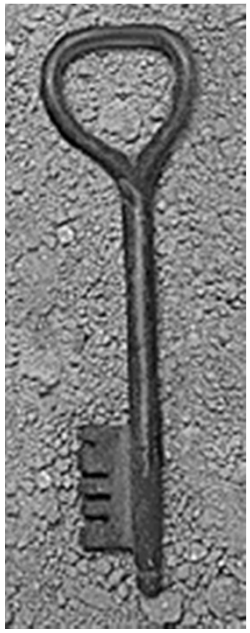


Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address

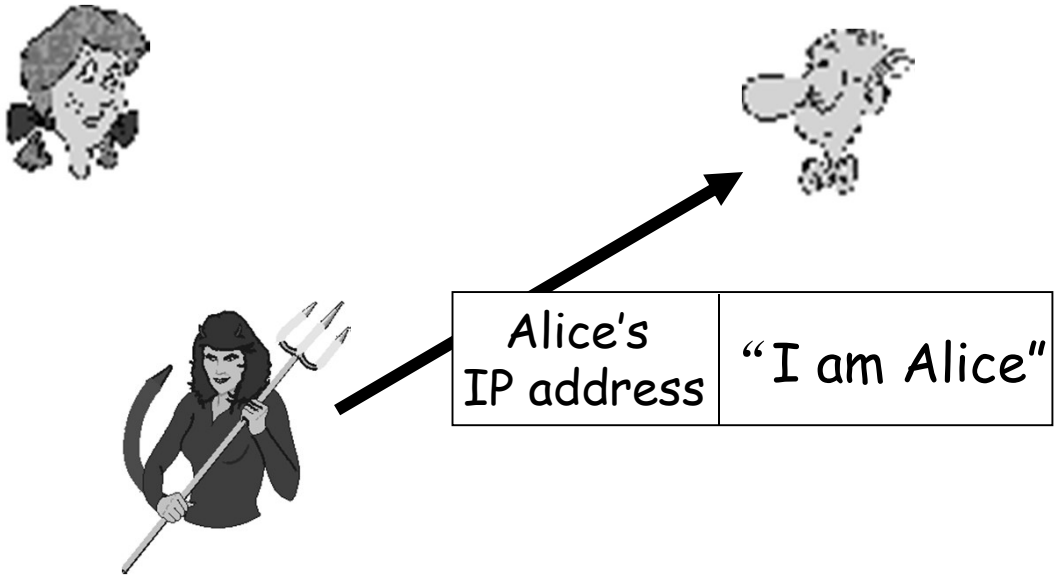


Failure scenario??

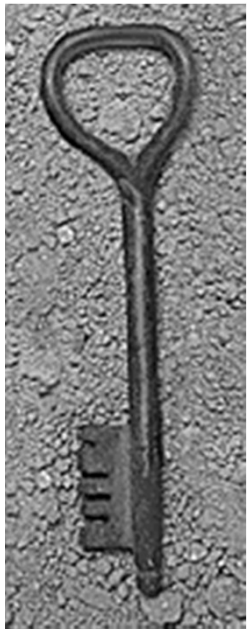


Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address

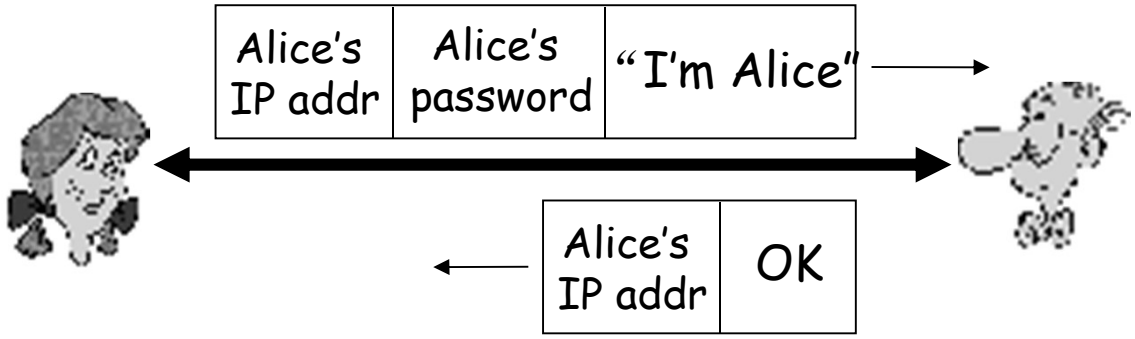


Trudy can create a packet "spoofing" Alice's address

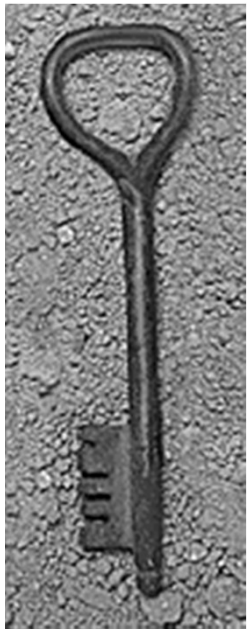


Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.

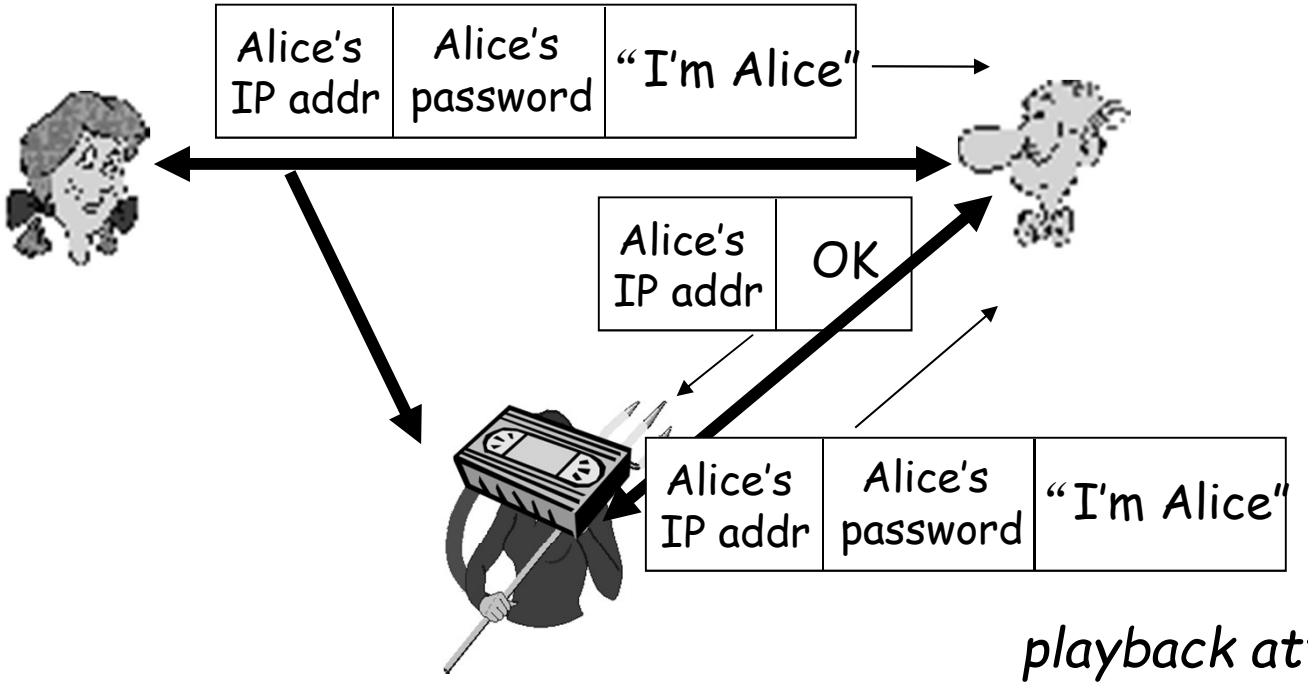


Failure scenario??

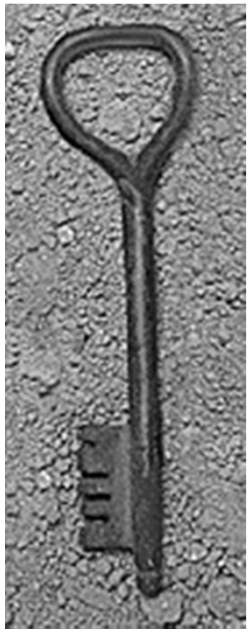


Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.

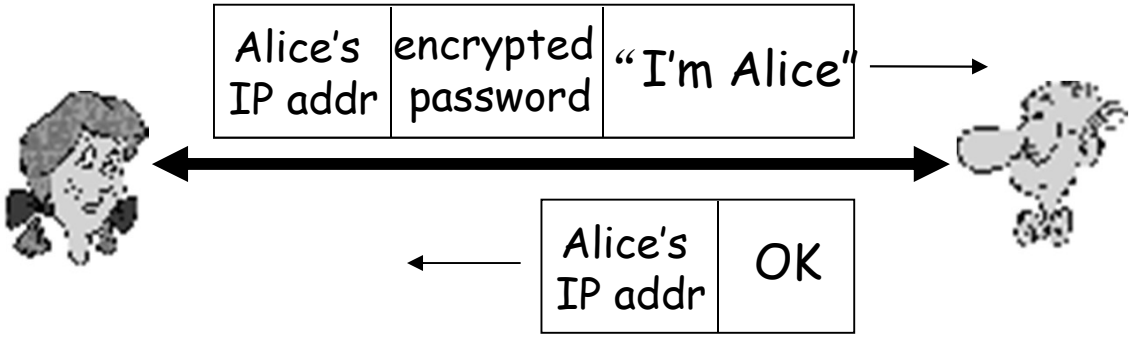


playback attack: Trudy records Alice's packet and later plays it back to Bob

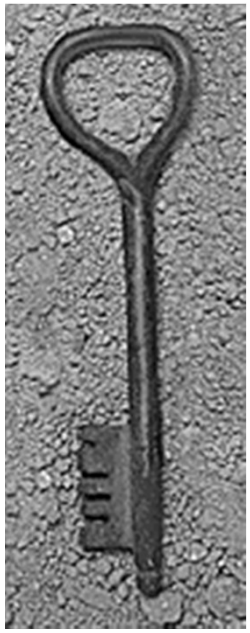


Authentication: yet another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.

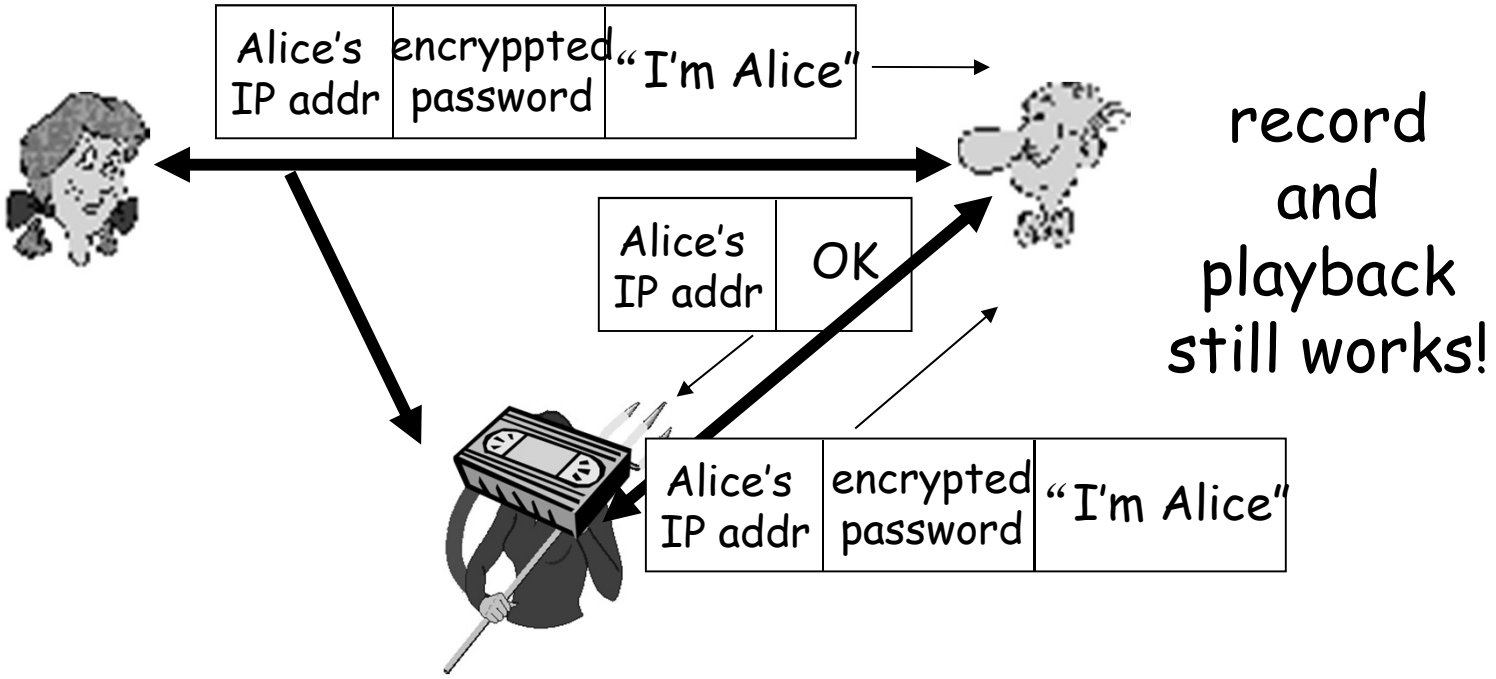


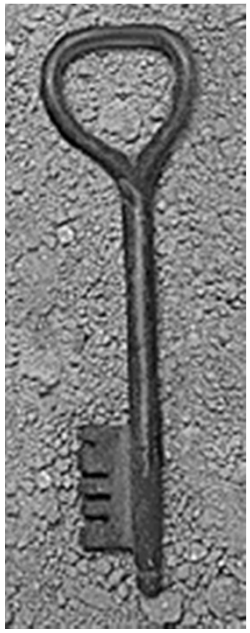
Failure scenario??



Authentication: another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



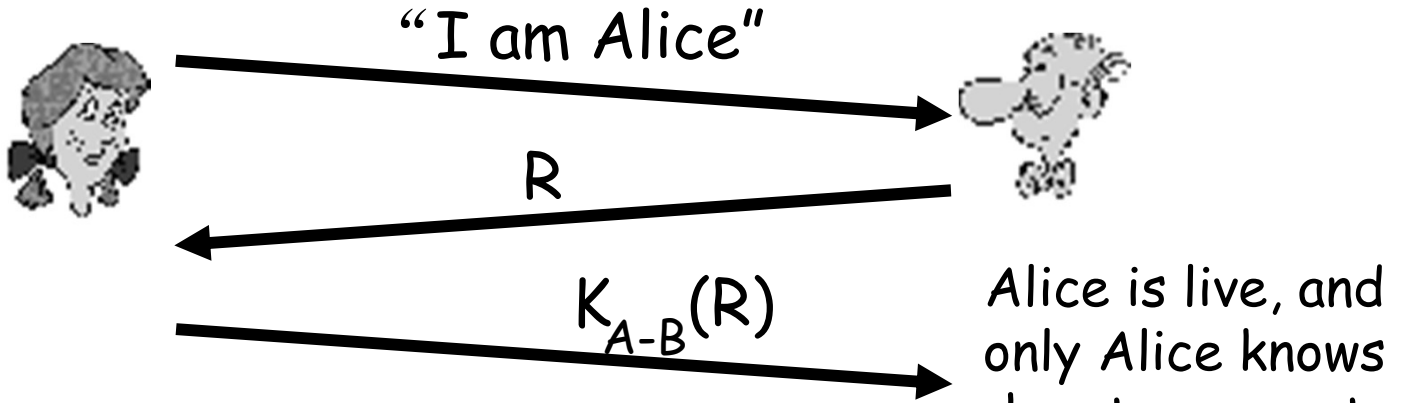


Authentication: yet another try

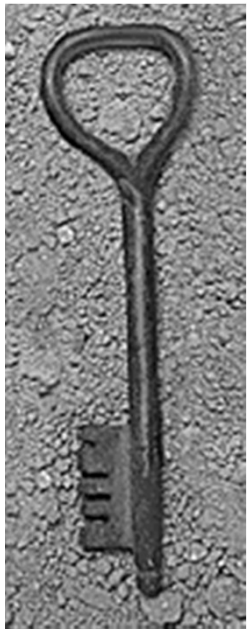
Goal: avoid playback attack

Nonce: number (R) used only *once –in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice nonce R, Alice must return R, encrypted with shared secret key



Failures, drawbacks?

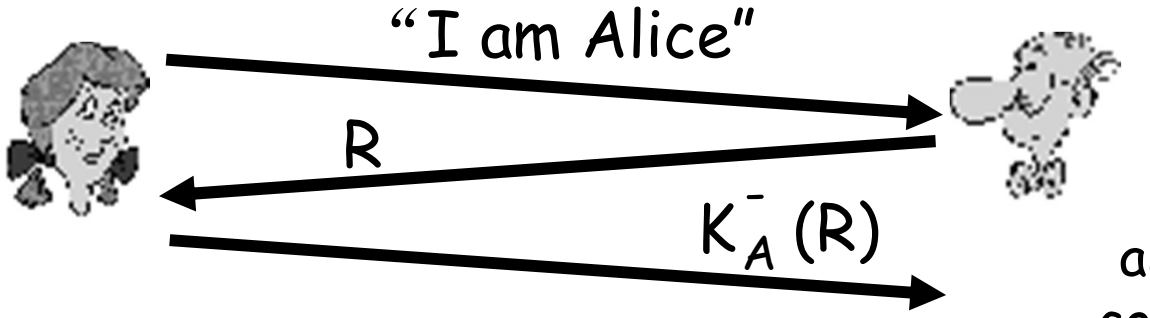


Authentication: ap5.0

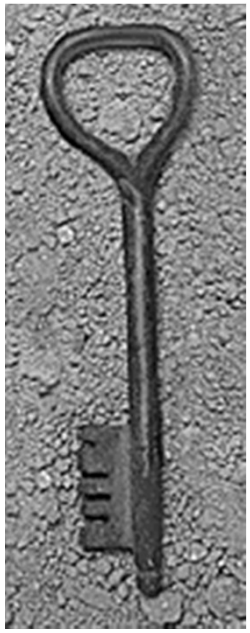
ap4.0 doesn't protect against server database reading

- can we authenticate using public key techniques?

ap5.0: use nonce, public key cryptography

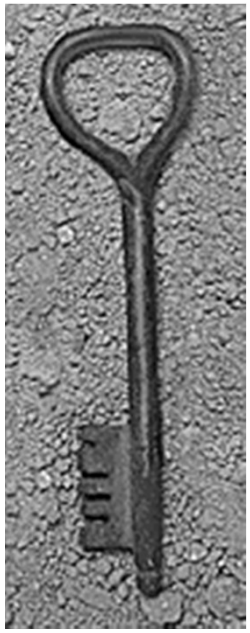


Bob computes
$K_A^+(K_A^-(R)) = R$
and knows only Alice could have the private key, that encrypted R such that
$K_A^+(K_A^-(R)) = R$



Agenda

- Basic Concepts
- Password-Based Authentication
- Biometrics
- Authentication Protocols
- Advanced Topic: Graphical Passwords



Advanced Topics: Graphical Passwords

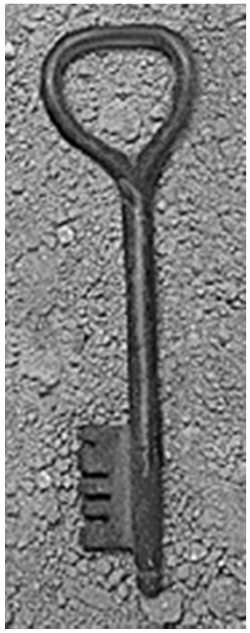
- Images are easy for humans to process and remember
  - Especially if you invent a memorable story to go along with the images
- Dictionary attacks on graphical passwords are difficult
  - Images are believed to be very "random" (is this true?)
- Still not a perfect solution
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

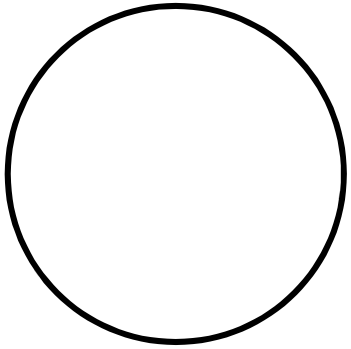
Passfaces Meets the Challenge

Secure and Usable

From Advertising
Materials, FYI only!

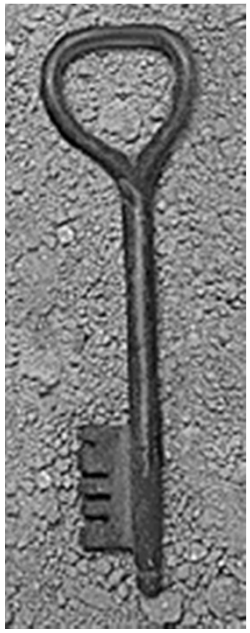
The Brain Deals with Faces Differently than Any Other Image





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, Cued Recall vs. Recognize

Three forms of memory

You must RECALL a password

You simply RECOGNIZE a face

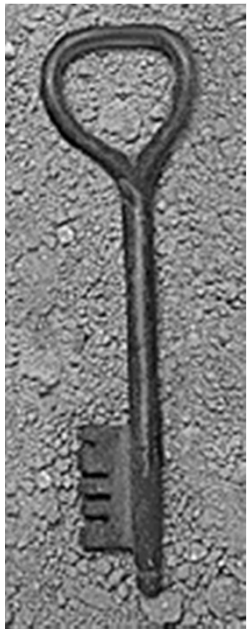
REMEMBER High School ….
(Cued recall)

Fill in the Blank

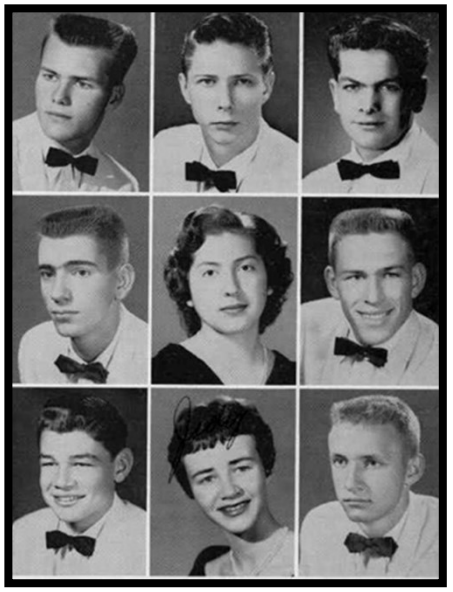
1 2 3 g y

What kind of test did your prefer?

Multiple Choice



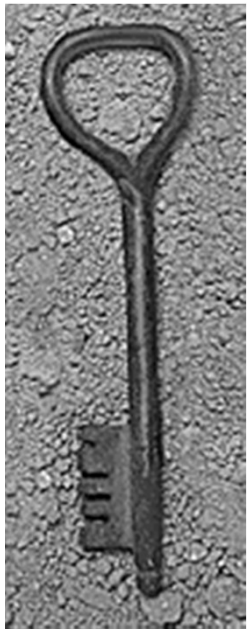
We Never Forget a Face



Think about how many people you already recognize.

Why wouldn't you remember your Passfaces?

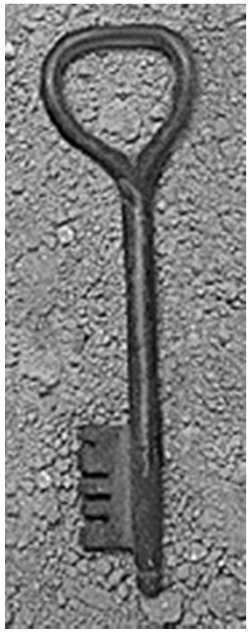
- *"Haven't used Passfaces in 6 months. I decided to take another look at it and, amazingly, I logged right in!"*
- *In one major government installation, there have been no forgotten Passfaces in over three years. The more its used, the easier it gets.*



Our approach

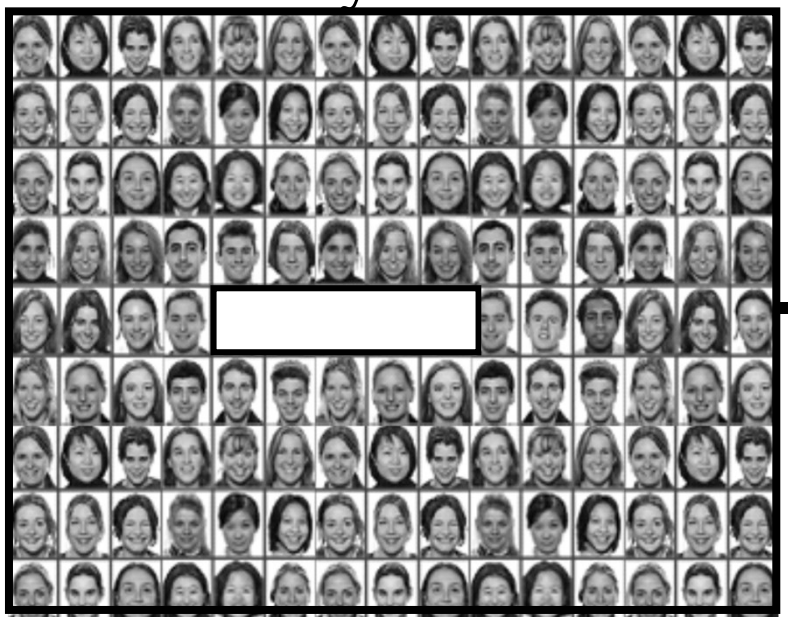
Familiarize the user with a randomly-selected set of faces and check if they can recognize them when they see them again

It's as easy as recognizing an old friend



How Passfaces Works

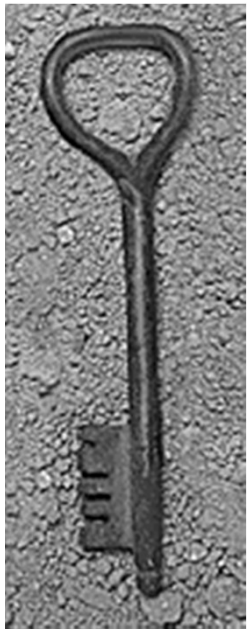
Library of Faces



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

Familiarization Puts Cookies in the Brain

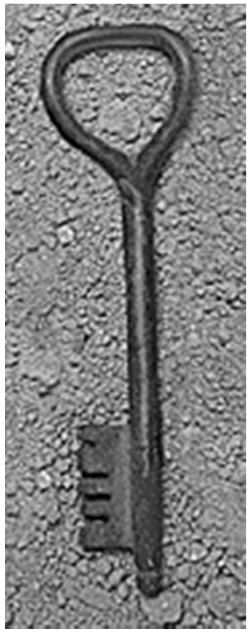
Like a *mindprint* or *brain cookie*

But, unlike fingerprints,

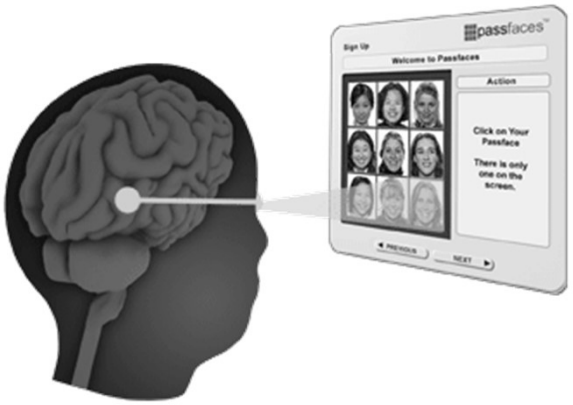
Passfaces require no special hardware

And, unlike browser cookies,

Passfaces authenticate the actual user



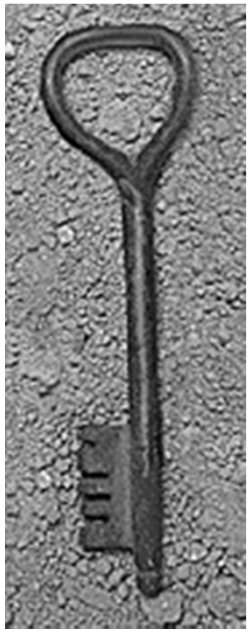
A New Class of Authentication



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

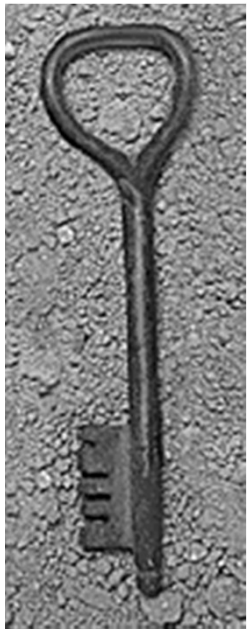
Cognometrics

Recognition-Based Authentication



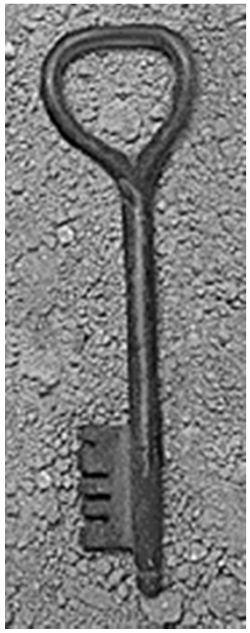
Empirical Results

- 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



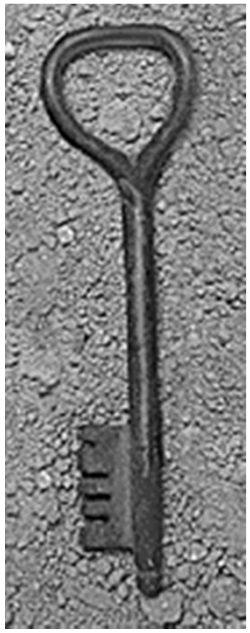
User Quotes

- *"I chose the images of the ladies which appealed the most"*
- *"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"*



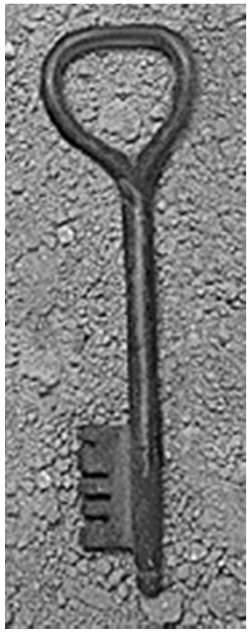
Other Images / Image Sequences?

Invent a story for an image
or a sequence of images

"We went for a walk
in the park yesterday"

girl-fish-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"
- Picture selection biases
  - Males select nature and sports more than females
  - Females select food images more often