CSE 410/565: Computer Security

Instructor: Dr. Ziming Zhao

Announcements

- HW-1 posted on UBLearns; due on March 2nd 11:59PM
- The instructor will be out of town on the 27th (Next Monday). Instead, the class will be delivered online on the 24th 9PM. Students can attend the online session though it is not required. Recording will be provided thereafter.

Authentication I

Authentication

- Message Authentication
  - Message Authentication Code (Keyed Hash) to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity).

- User/entity Authentication
  - Allow a user/computer to prove his/her/its identity to another entity (e.g., a system, a device).

User/entity Authentication

- Authentication is a broad term and is normally referred to mechanisms of ensuring that
  - entities are who they claim to be
  - data has not been manipulated by unauthorized parties
- User/entity authentication or identification refers to the means of verifying user identity
  - if such verification is successful, the user is granted appropriate privileges
- The need for user authentication in early computer systems arose once it became possible to support multi-user environments

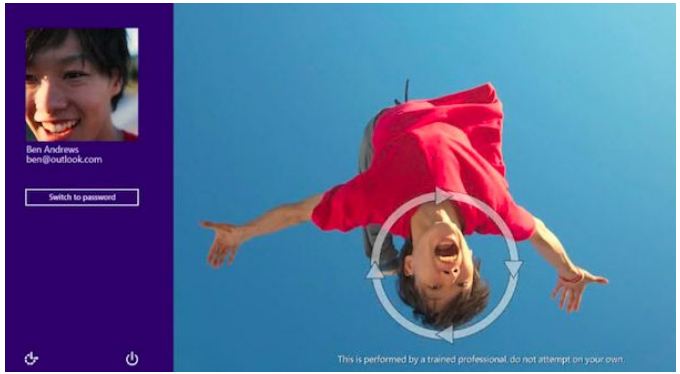
Entity Authentication

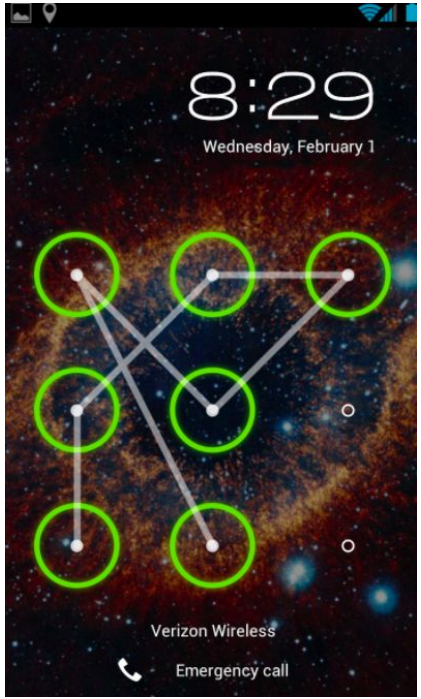
- During an authentication protocol:
  - one party, the verifier, gathers evidence that the identity of another party, the claimant, is as claimed
- Goals of authentication protocols:
  - honest parties should be able to successfully finish the protocol with their identity accepted as authentic
  - it should be difficult for dishonest parties to impersonate an identity of another user
  - impersonation must remain difficult even after observing a large number of successful authentications by other parties
- User registration is required prior to an authentication protocol

Entity Authentication

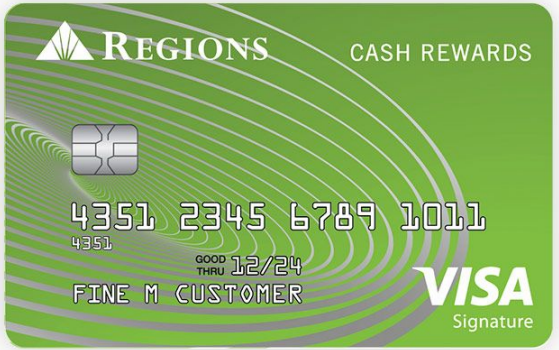
- Identification mechanisms are often divided into 3 types based on how the identity evidence is gathered
  - user knows a secret
    - examples include passwords, personal identification numbers (PINs), secret keys, mother's maiden name, etc.
  - user possesses a token
    - these are normally hardware tokens such as magnetic-striped cards or custom-designed devices for time-variant passwords
  - user has a physical attribute
    - characteristics inherent to the user such as biometrics, handwritten signatures, keystroke dynamics, facial and hand geometries, voice, etc.

User knows a secret

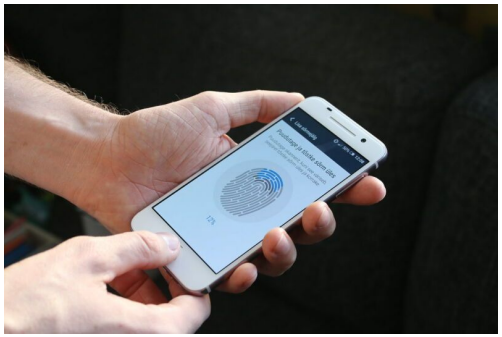


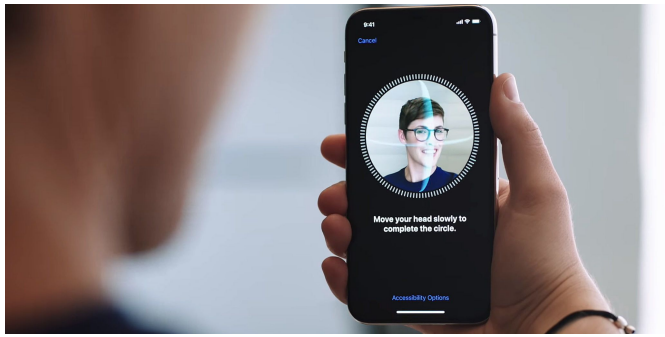


User possesses a token

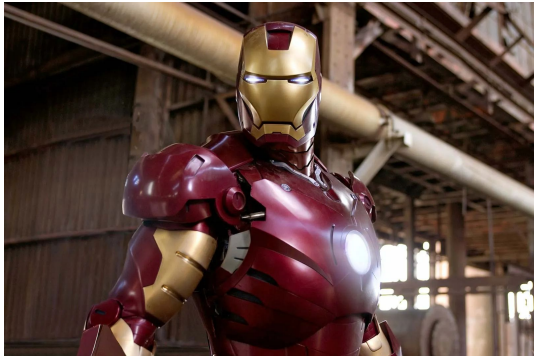


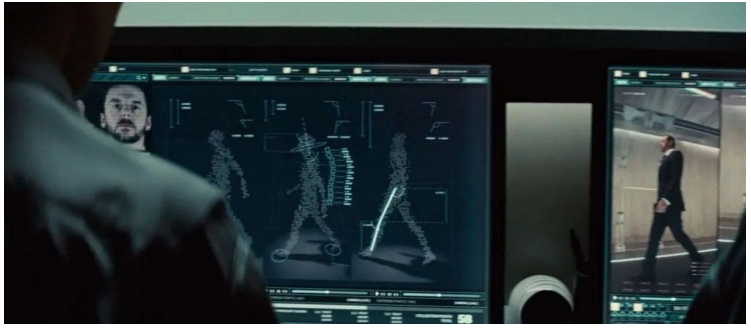
User has a physical attribute (biometrics)

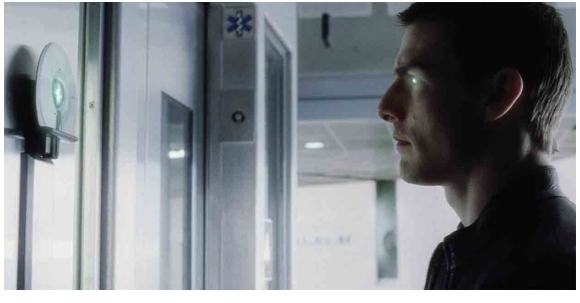




User has a physical attribute (biometrics)







Entity Authentication

- Often, different types can be combined together
  - e.g., PIN-based authentication is often used with a physical device (user ID, credit card)
  - biometric-based authentication is often used in combination with a password or a physical token
- Many identification mechanisms used in practice are not secure
  - calling cards
  - credit card purchases
  - Passwords
- Ideally we want solutions against which replay attacks don’t work

Password-Based Authentication

- A password is a string of characters associated with a certain user
  - it serves the purpose of a shared secret between the user and the system
- During the identification protocol:
  - a user sends (*userid*, *password*) pair
    - *userid* identifies the user
    - password provides the necessary evidence that the user possesses the secret
  - the system compares that information with its has stored
  - if the check succeeds, access is granted

Password-Based Authentication

- Storage of passwords
  - the most straightforward way of storing passwords is in clear text
    - there is a problem with such approach
  - to mitigate it, most systems apply a password-hash function to a password and store the hash
    - the password itself cannot be recovered, but there are other concerns
- Attacks on passwords
  - replay of passwords: an attacker reuses a captured password
    - an attacker can capture a password by seeing a user type it, using a keylogger program or obtaining it in transit

Password-Based Authentication

- Attacks on passwords (cont.)
  - exhaustive search: an attacker attempts to guess a user password by trying all possible strings
    - this can be done on the verifier itself or by obtaining a copy of the password file and performing the attack off-line
    - often the attack is infeasible if the password space is large enough
      - but it is still possible to exhaust all short passwords
  - dictionary attack: an attacker tries to guess a password using words from a dictionary and variations thereof
    - can have a high probability of success
    - dictionary attacks become increasingly sophisticated

Password-Based Authentication

- Is there a way to decrease the vulnerability of the system to such attacks?
- Additional measures are normally employed, some of which are:
  - salting passwords
    - this technique makes guessing attacks less effective
    - a password is augmented with a random string, called salt, prior to hashing
    - the salt is stored in cleartext in the password file

$$uid_1, salt_1, h(salt_1||pwd_1)$$

$$uid_2, salt_2, h(salt_2||pwd_2)$$

    - how does it improve security?

Password-Based Authentication

- Measures for improving security of passwords (cont.)
  - slowing down password verification
    - the hash function for password verification is made more computationally extensive
    - this can be done, e.g., by iterating the computation n times
  - limiting the number of unsuccessful password guesses
    - a user account is locked after the number of successive unsuccessful authentication attempts exceeds the threshold
  - employing password rules
    - additional rules on password choices are imposed
    - this often strengthens password choices but limits the search space

Password-Based Authentication

- Measures for improving security of passwords (cont.)
  - preventing direct access to password file
    - the file/database with hashed passwords is kept inaccessible by ordinary users
- Another technique that aims at improving security of passwords is called password aging (enforce the regular changing of passwords)
- It is always a challenge to find a balance between memorability of passwords and their resistance to dictionary attacks
  - do users make acceptable password choices?
  - can we help them with choosing strong passwords?

Password-Based Authentication

- Password strength has been studied since 1990s
  - a significant portion of used passwords is guessable
    - passwords of short length can be cracked using brute force search
    - account-related or dictionary-derived passwords are common
  - password crackers today are increasingly complex
- How can we help users to select stronger passwords?
  - systems are much better at helping users than before
  - a variety of tools exist

Password-Based Authentication

- User-chosen secrets
- Suppose passwords could be up to 9 characters long
- This would produce 10^18 possible passwords
- 320,000 years to try them all at 10 million a second!

- Unfortunately, not all passwords are equally likely to be used
  - Users have the tendency to choose easy to remember but weak password

Password-Based Authentication

The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis

Yinqian Zhang
University of North Carolina at Chapel Hill
Chapel Hill, NC
yinqian@cs.unc.edu

Fabian Monrose
University of North Carolina at Chapel Hill
Chapel Hill, NC
fabian@cs.unc.edu

Michael K. Reiter
University of North Carolina at Chapel Hill
Chapel Hill, NC
reiter@cs.unc.edu

Password-Based Authentication

- Tools for choosing stronger passwords
  - computer-generated passwords
    - selecting less predictable passwords which users can remember can be done by using computer-generated pronounceable passwords
    - for example: heloberi, hoparmah, ulensoev, atonitim
  - password checking
    - a proactive password checker rates password strength at the time of password selection
  - other types of passwords
    - techniques for using images and graphical interfaces for authentication have been developed

Password-Based Authentication

- Tools for choosing stronger passwords (cont.)
  - image-based passwords and graphical interfaces
  - displaying a sequence of images
  - drawing patterns on a grid
  - choosing points using an image
  - their unpredictability is often not as great as desired
- Unpredictability and usability of passwords is hard to achieve simultaneously
  - passwords can provide only a weak form of security

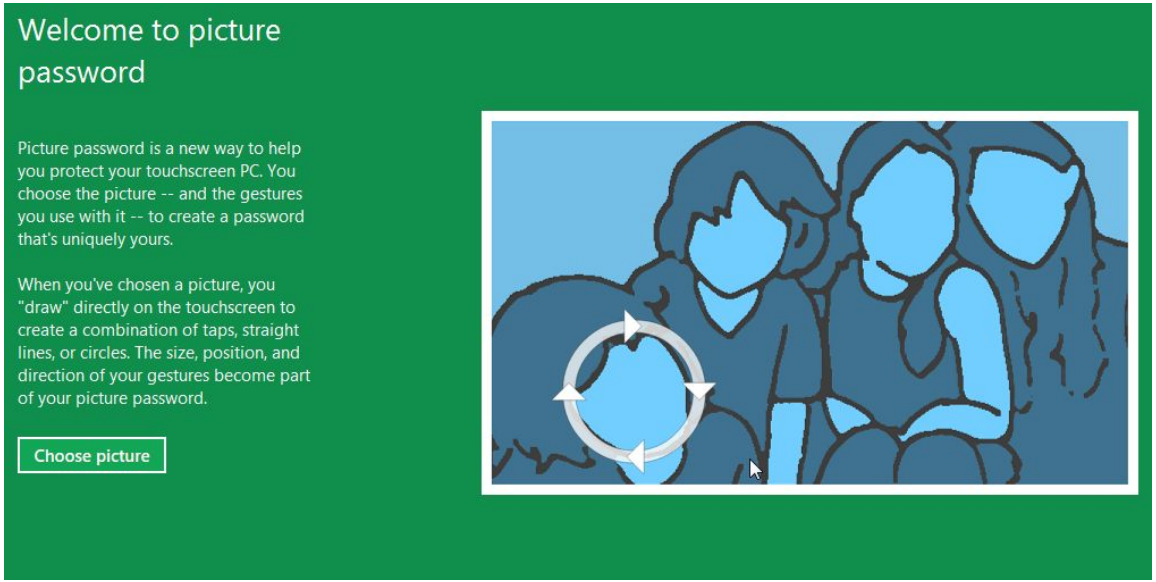
Best Password Practices

- NIST's Special Publication 800-63 provides authentication guidelines for organizations including password-based authentication
  - the latest version is dated by June 2017
- In general, you want to
  - use strong passwords
  - not reuse passwords across different services
  - not share your passwords with anyone else
- Password managers are of great help in dealing with password explosion

Picture Password as an Example

Picture Gesture Authentication (PGA)

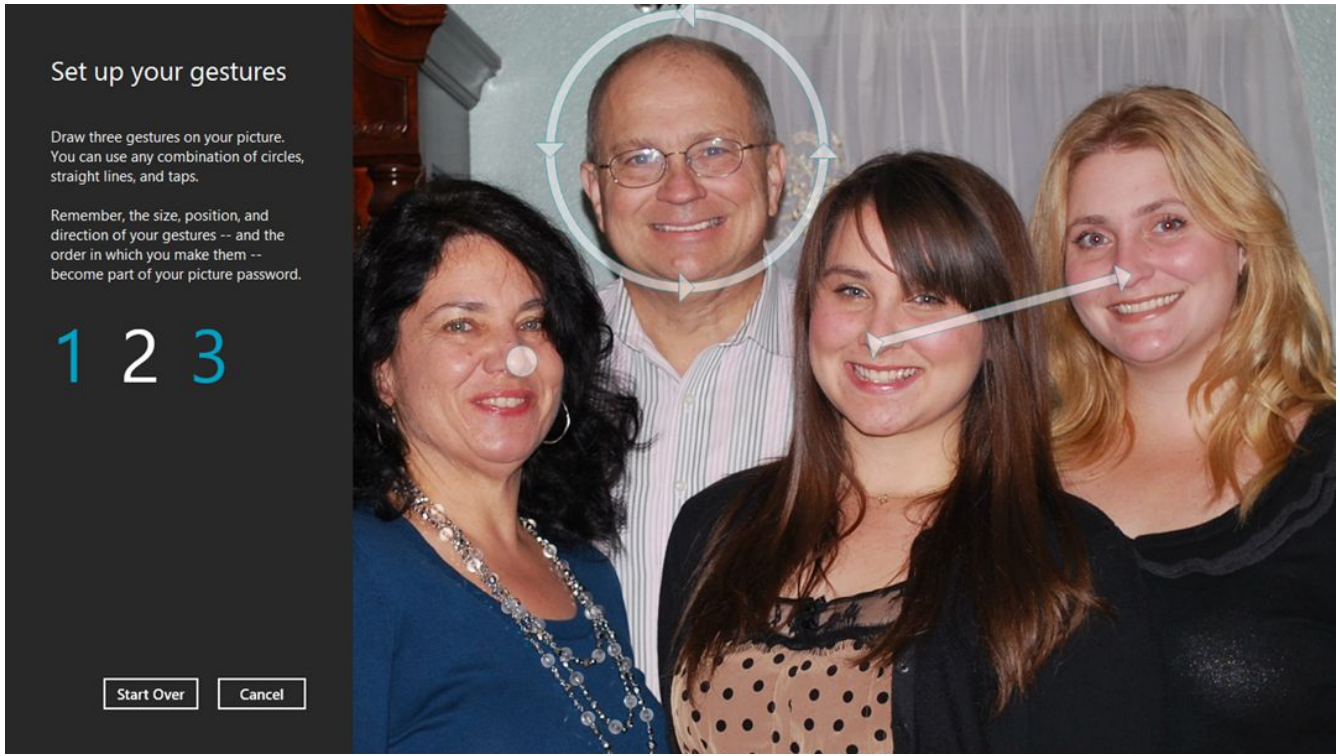
A built-in feature in Microsoft Windows 8



How PGA works

Three types of gestures are allowed

- Tap
- Circle
- Line



Research Questions

How to understand user-choice patterns in PGA?

- Background Pictures
- Gesture Location
- Gesture Type
- Gesture Order

How to use these patterns to guess PGA password?

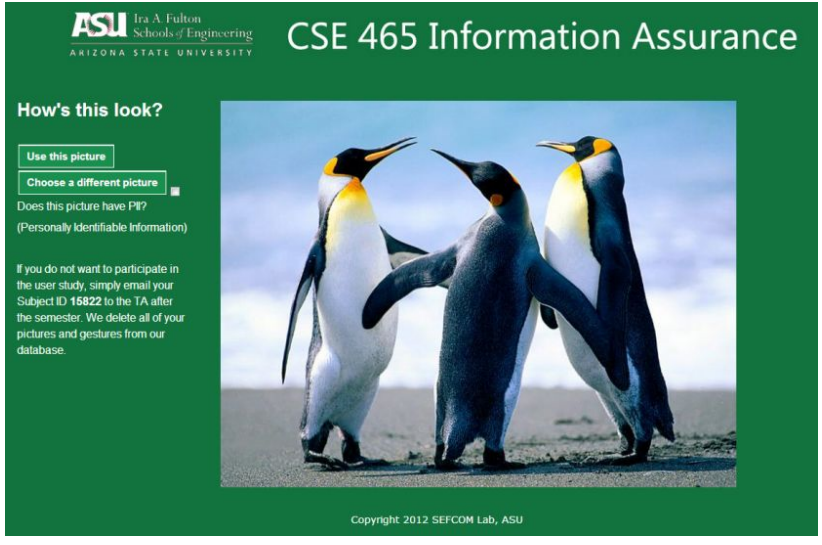
Part 1: User Studies

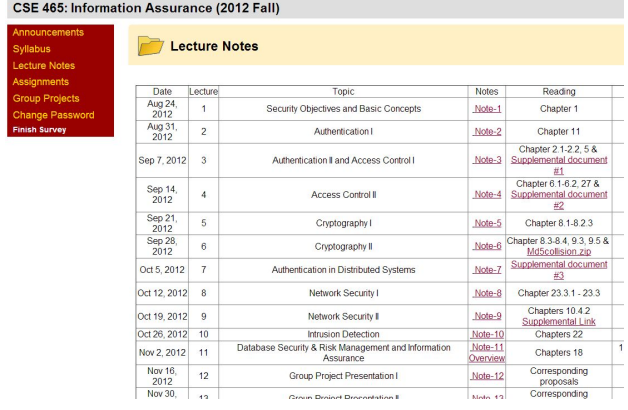
Web-based PGA system
- Similarity to Windows PGA
- Workflow
- Appearance

Data collection

Analysis: survey and results

Dataset-1
- ASU undergraduate computer security class (Fall 2012)
- 56 participants
- 58 unique pictures
- 86 passwords
- 2,536 login attempts



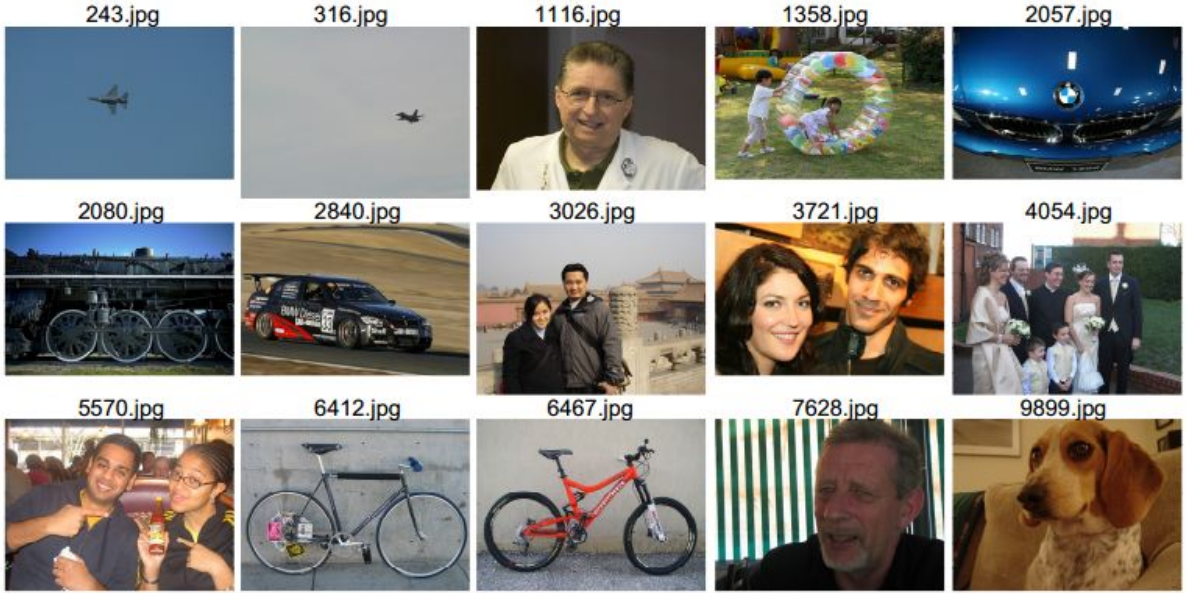


Date	Lecture	Topic	Notes	Reading
Aug 24, 2012	1	Security Objectives and Basic Concepts	Note-1	Chapter 1
Aug 31, 2012	2	Authentication I	Note-2	Chapter 11
Sep 7, 2012	3	Authentication II and Access Control I	Note-3	Chapter 2.1-2.2, 5 & Supplemental document #1
Sep 14, 2012	4	Access Control II	Note-4	Chapter 6.1-6.2, 27 & Supplemental document #2
Sep 21, 2012	5	Cryptography I	Note-5	Chapter 8.1-8.2.3
Sep 28, 2012	6	Cryptography II	Note-6	Chapter 8.3-8.4, 9.3, 9.5 & MdSollision.zip
Oct 5, 2012	7	Authentication in Distributed Systems	Note-7	Supplemental document #3
Oct 12, 2012	8	Network Security I	Note-8	Chapter 23.3.1 - 23.3
Oct 19, 2012	9	Network Security II	Note-9	Chapters 10.4.2 Supplemental Link
Oct 26, 2012	10	Intrusion Detection	Note-10	Chapters 22
Nov 2, 2012	11	Database Security & Risk Management and Information Assurance	Note-11 Overview	Chapters 18
Nov 16, 2012	12	Group Project Presentation I	Note-12	Corresponding proposals
Nov 30,	13	Group Project Presentation II	Note-13	Corresponding

Part 1: User Studies

Dataset-2

- Scenario: The password is used to protect your bank account
- Amazon MTurk
- 15 pictures selected in advance
- 762 participants
- 10,039 passwords



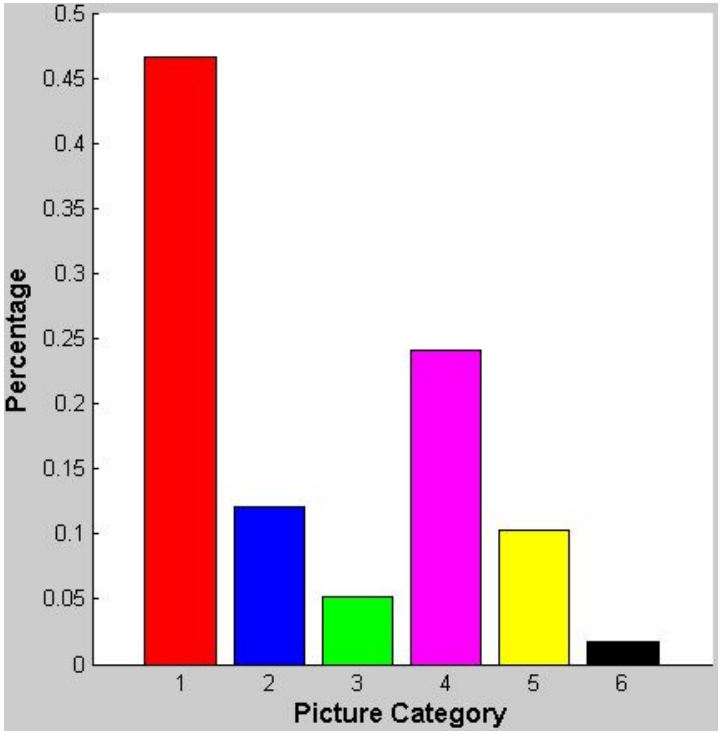
Part 1: User Studies

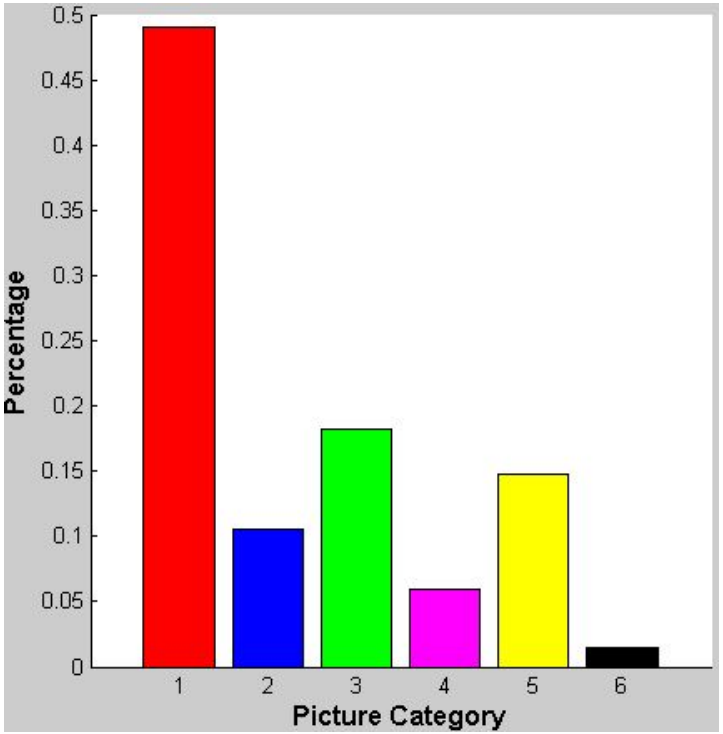
Survey questions

- General information of the subject
- General feeling towards PGA
- How she/he selects a background picture
- How she/he selects a password

Part 1: User-choice Patterns
Background Picture

People, Civilization, Landscape, Computer-generated, Animal, Others





Part 1: User-choice Patterns
Why or why not picture of people

- Advocates:
  - it is more friendly
    - ‘The image was special to me so I enjoy seeing it when I log in’
  - it is easier for remembering passwords
    - ‘Marking points on a person is easier to remember’
  - it makes password more secure
    - ‘The picture is personal so it should be much harder for someone to guess the password’

- Others:
  - leak his or her identify or privacy
    - ‘revealing myself or my family to anyone who picks up the device’

Part 1: User-choice Patterns
Gesture Locations

- Which of the following best describes what you are considering when you choose locations to perform gestures?

	Dataset-1	Dateset-2
I try to find locations where special **objects** are.	72.7%	59.6%
I try to find locations where some special **shapes** are.	24.2%	21.9%
I try to find locations where **colors** are different from their surroundings.	0%	8.7%
I randomly choose a location to draw without thinking about the background picture.	3.0%	10.1%

Part 1: User-choice Patterns
Gesture Locations

- Which of the following best describes what you are considering when you choose locations to perform

Most users tend to draw passwords on Points-of-Interest (PoIs) in the background picture.

are.

I try to find locations where **colors** are different from their surroundings.	0%	8.7%
I randomly choose a location to draw without thinking about the background picture.	3.0%	10.1%

Part 1: User-choice Patterns
Gesture Locations (Picture of People)

- Dataset-1
  - 22 subjects uploaded 27 pictures of people
  - 31 passwords (93 gestures)

Attributes	# Gesture	# Password	# Subject
Eye	36 (38.7%)	20 (64.5%)	19 (86.3%)
Nose	21 (22.5%)	13 (48.1%)	10 (45.4%)
Hand/ Finger	6 (6.4%)	5 (18.5%)	4 (18.2%)
Jaw	5 (5.3%)	3 (11.1%)	3 (13.7%)
Face	4 (4.3%)	2 (7.4%)	2 (9.1%)

Part 1: User-choice Patterns
Gesture Locations (Civilization)

Dataset-1

- Two versions of Starry Night uploaded by two participants

(a)

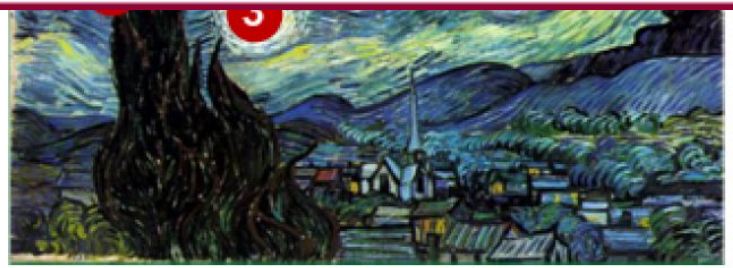
(b)

Part 1: User-choice Patterns
Gesture Locations (Civilization)

Dataset-1

- Two versions of Starry Night uploaded by two

Users have the tendencies to choose PoIs with the same attributes to draw on.



(a)

(b)

Part 1: User-choice Patterns
Windows PGA Advertisements

Asia

South America

Europe

Part 2: Attack Framework

- To generate dictionaries that have potential passwords
  - Picture-specific dictionary
  - Rank passwords with likelihood
  - Work on previously unseen pictures

- Our approach
  - Automatically learns user-choices patterns in the training pictures and corresponding passwords
  - Then applies these patterns to the target picture for dictionary generation

Part 2: Attack Framework
Selection Function

- Selection function
  - Models the password creating process that users go through
  - Takes two types of parameters
    - Gesture type, such as tap, circle, line
    - PoI attribute, such as face, eye, …
  - Generates a group of gestures

Part 2: Attack Framework
Selection Function (Examples)

*s: {tap,circle,line} x PoI Attributes**

s(circle, face): Circle a face in the picture

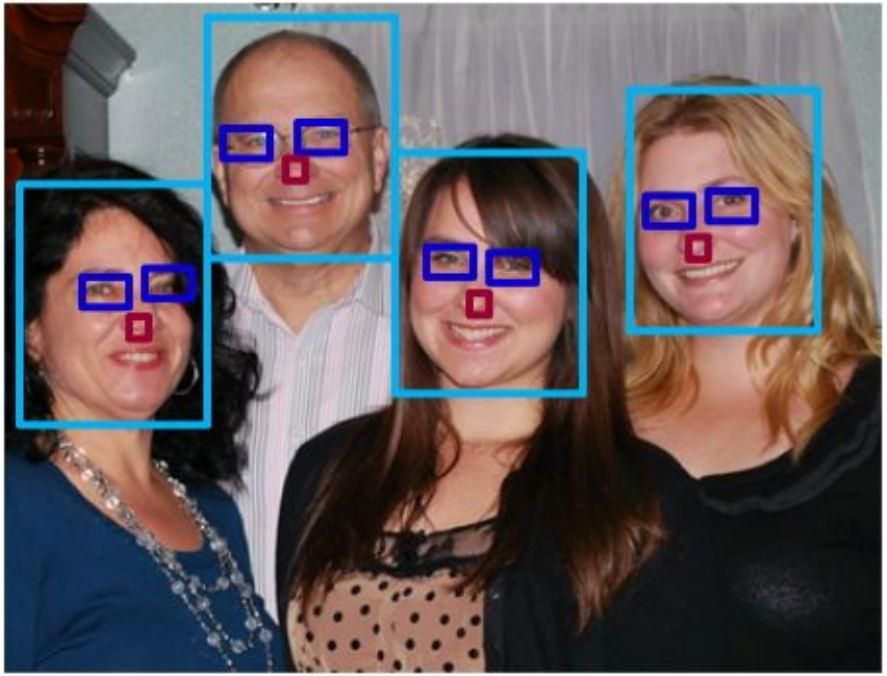
s(line, nose, nose): Line a nose to another nose in the picture

s(tap, nose): Tap a nose in the picture

Part 2: Attack Framework
Extract Selection Functions

Password

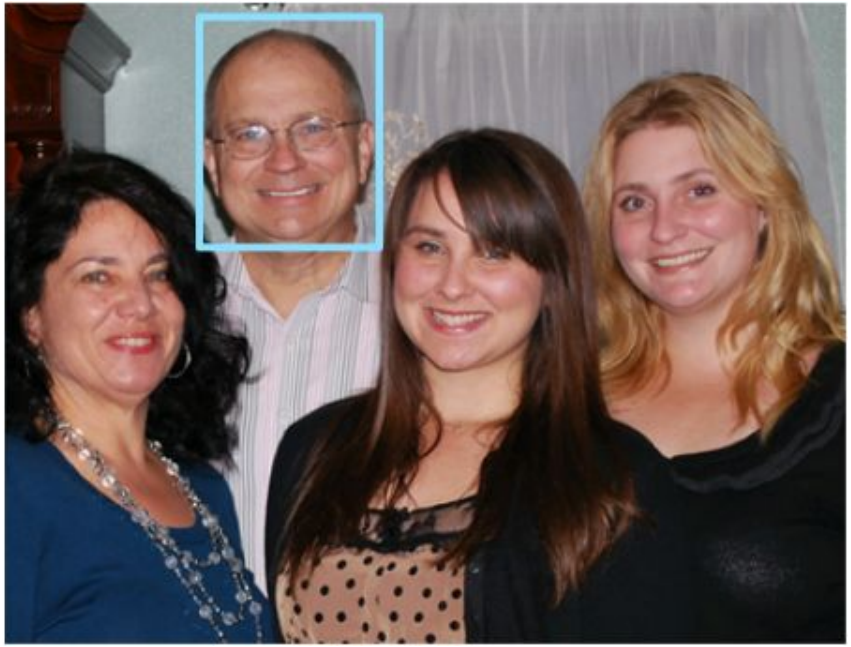
Points-of-Interest



Part 2: Attack Framework
Extract Selection Functions

Password

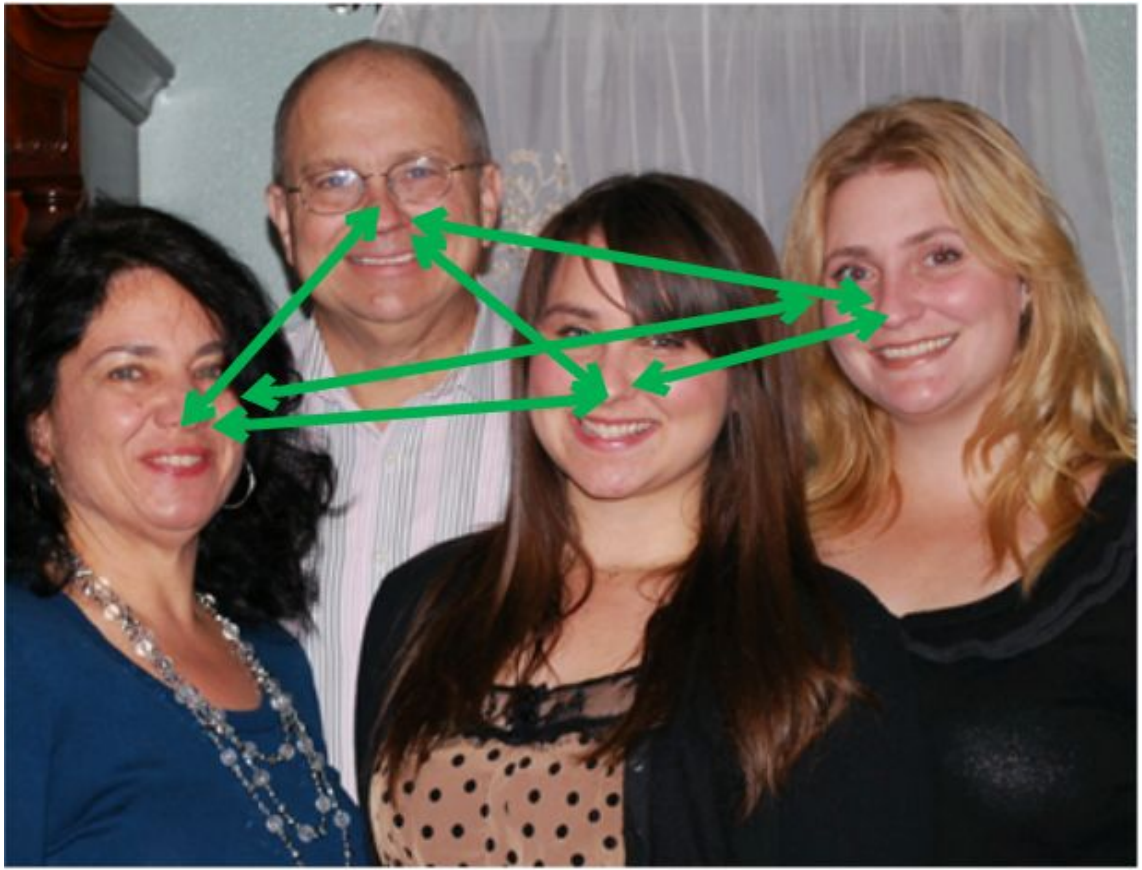
Points-of-Interest



Part 2: Attack Framework
Apply Selection Functions

Function 1:
s(circle, face)
Output: 4 gestures

Part 2: Attack Framework
Apply Selection Functions



Function 1:
s(circle, face)
Output: 4 gestures

Function 2:
s(line, nose, nose)
Output: 12 gestures

Part 2: Attack Framework
Apply Selection Functions

Function 1:
s(circle, face)
Output: 4 gestures

Function 2:
s(line, nose, nose)
Output: 12 gestures

Function 3:
s(tap, nose)
Output: 4 gestures

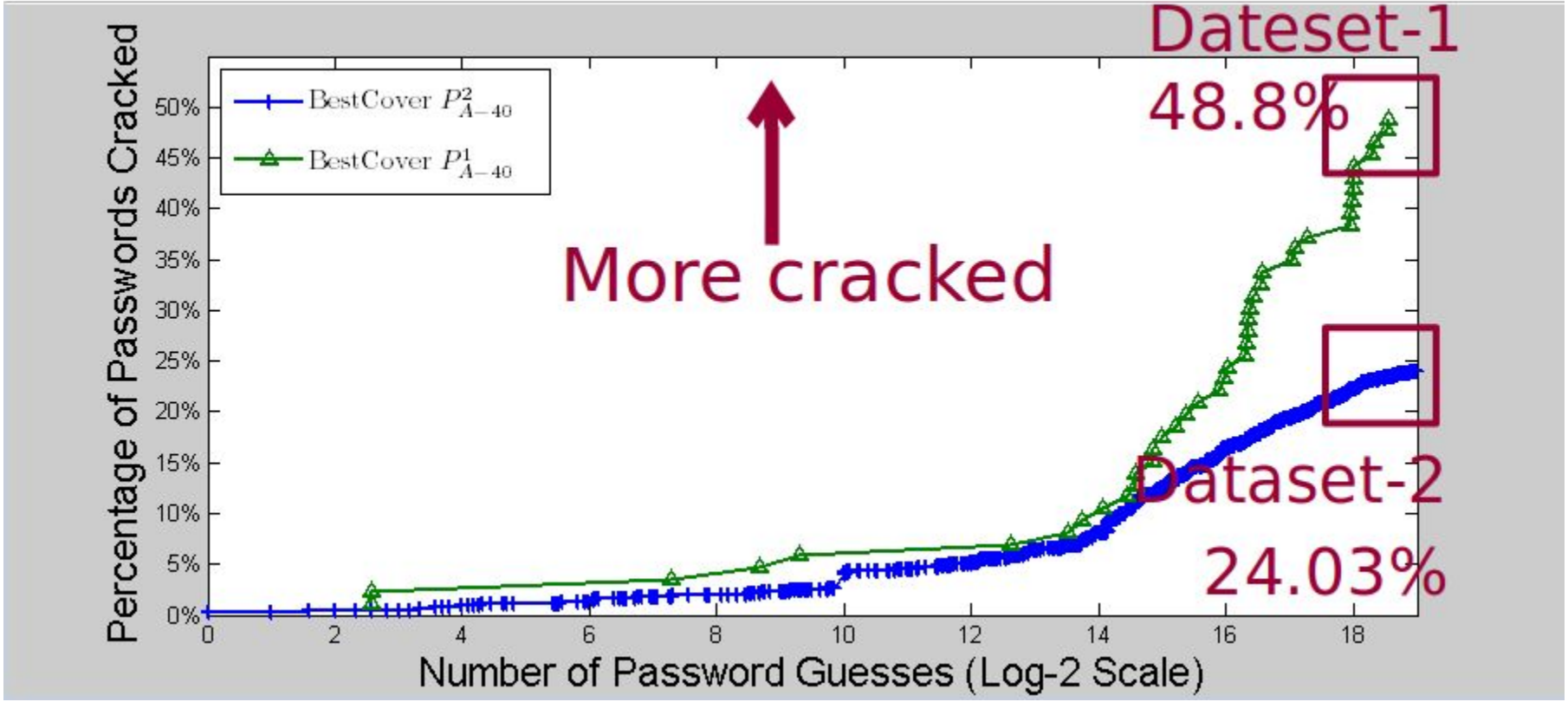
Number of potential passwords: 4×12×4 = 192

Part 2: Attack Framework
Rank Selection Functions

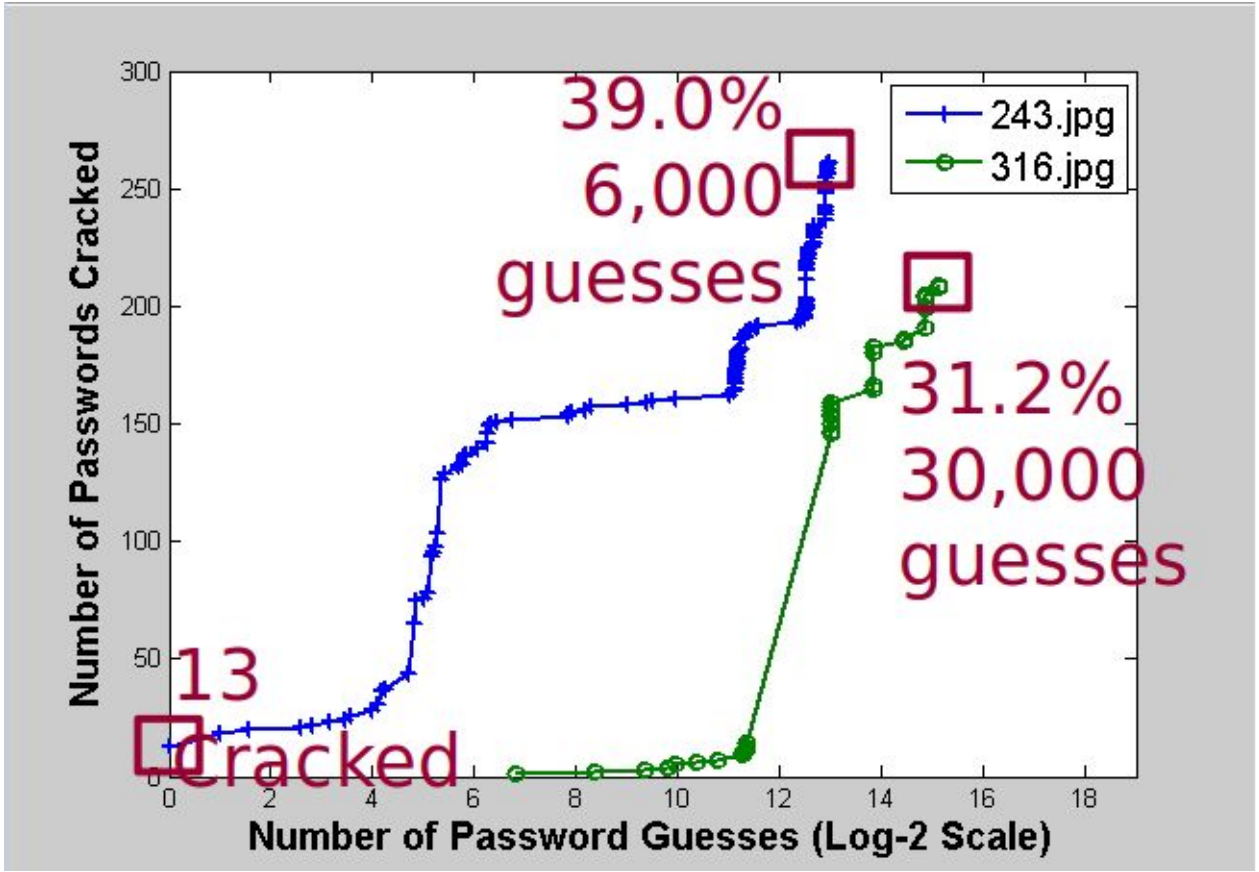
- BestCover algorithm
  - Derived from emts (Zhang et al. , CCS'10)
  - Optimizes guessing order for passwords in the training dataset

- Unbiased algorithm
  - Reduces the biased Points-of-Interest distributions in the training set

Part 3: Attack Results
Dateset-1 vs. Dateset-2

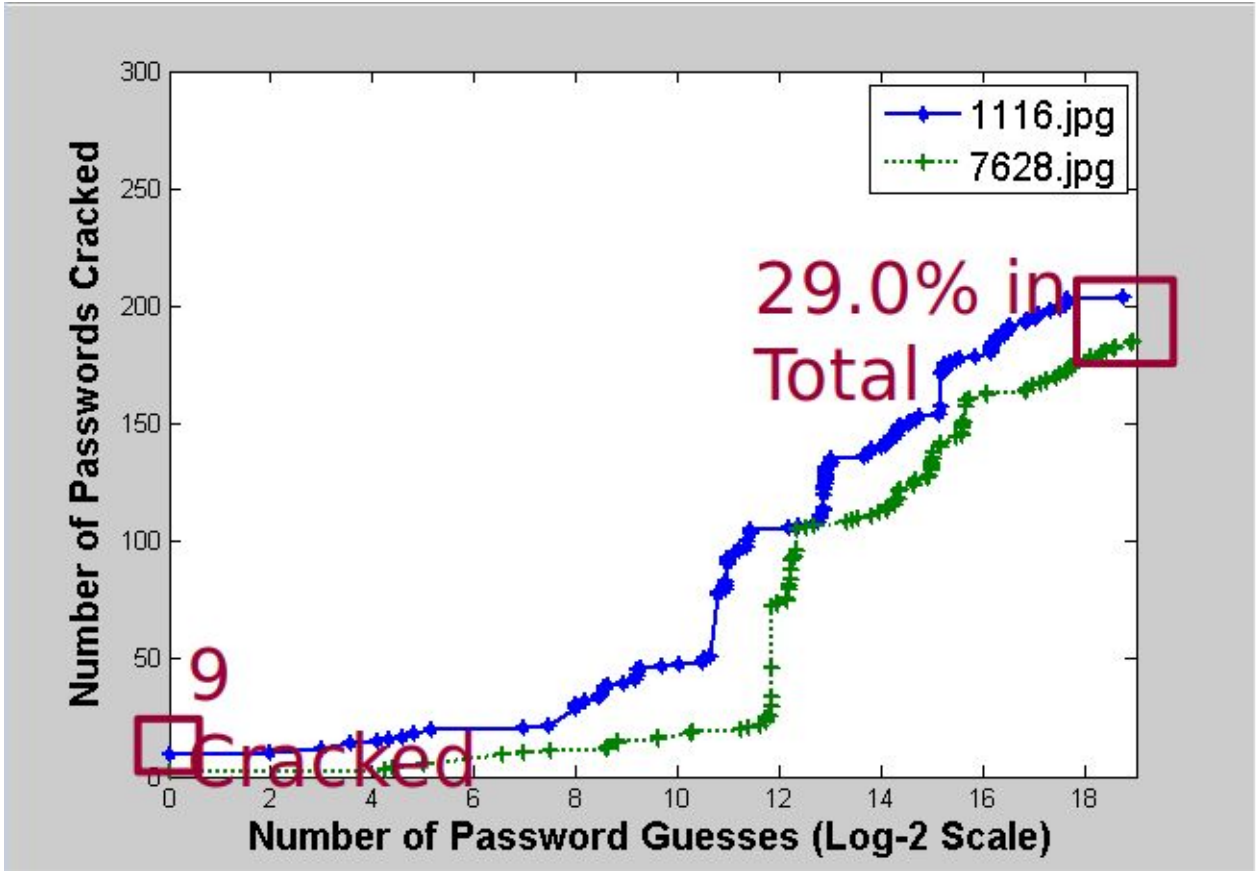


Part 3: Attack Results
Simple Pictures (Unbiased algorithm)



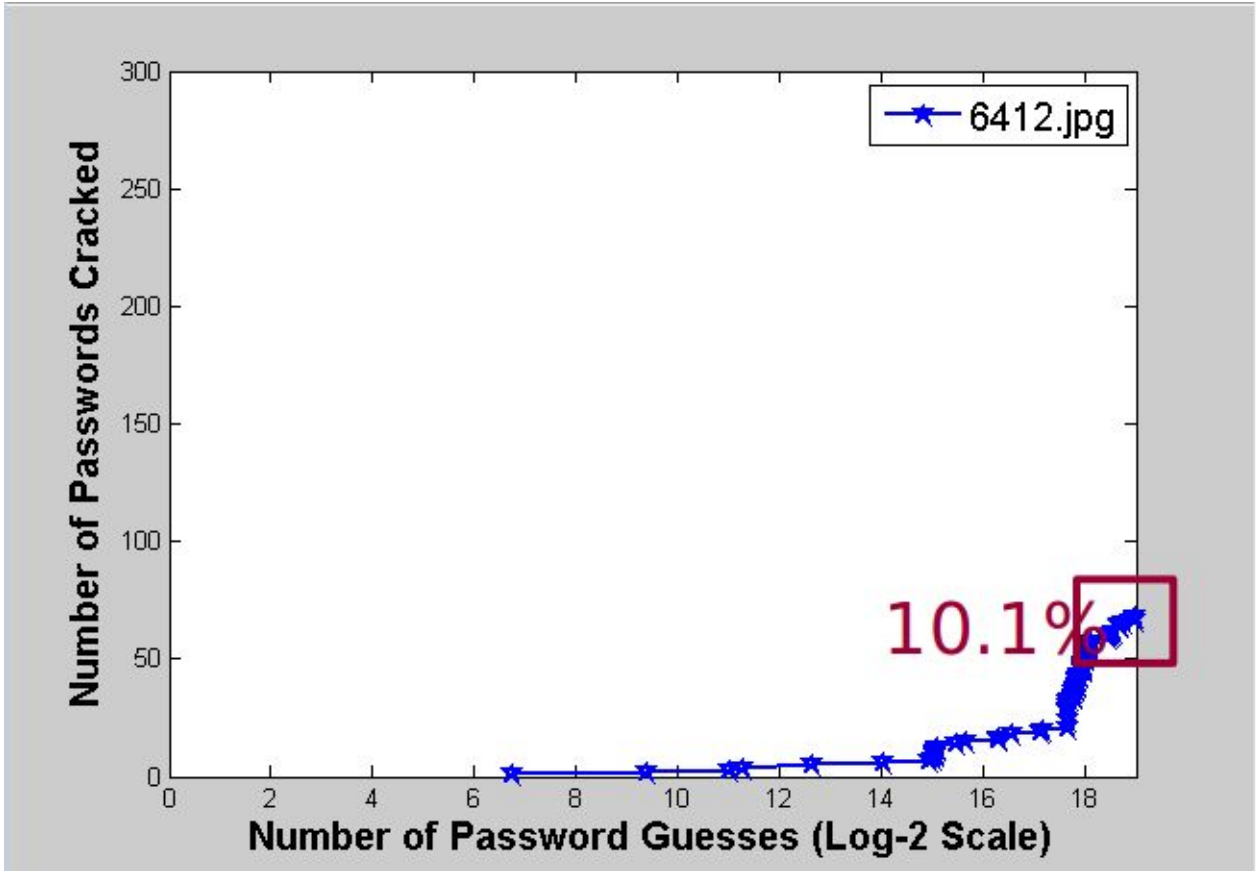
316.jpg

Part 3: Attack Results
Portraits (Unbiased algorithm)



7628.jpg

Part 3: Attack Results
Complex Picture (Unbiased algorithm)



6412.jpg