On the Security of Picture Gesture Authentication

Ziming Zhao[†‡], Gail-Joon Ahn[†‡], Jeong-Jin Seo[†], Hongxin Hu[§]

[†]Arizona State University [‡]GFS Technology [§]Delaware State University

Picture Gesture Authentication (PGA)

- A built-in feature in Microsoft Windows 8
- 60 million Windows 8 licenses have been sold
- 400 million computers and tablets will run Windows 8 in one year

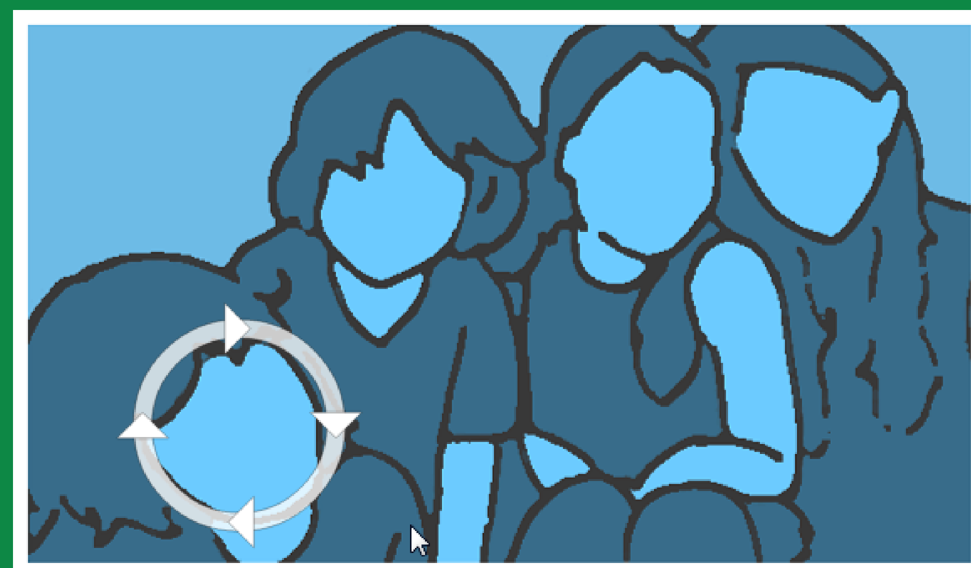
How PGA Works

Welcome to picture password

Picture password is a new way to help you protect your touchscreen PC. You choose the picture -- and the gestures you use with it -- to create a password that's uniquely yours.

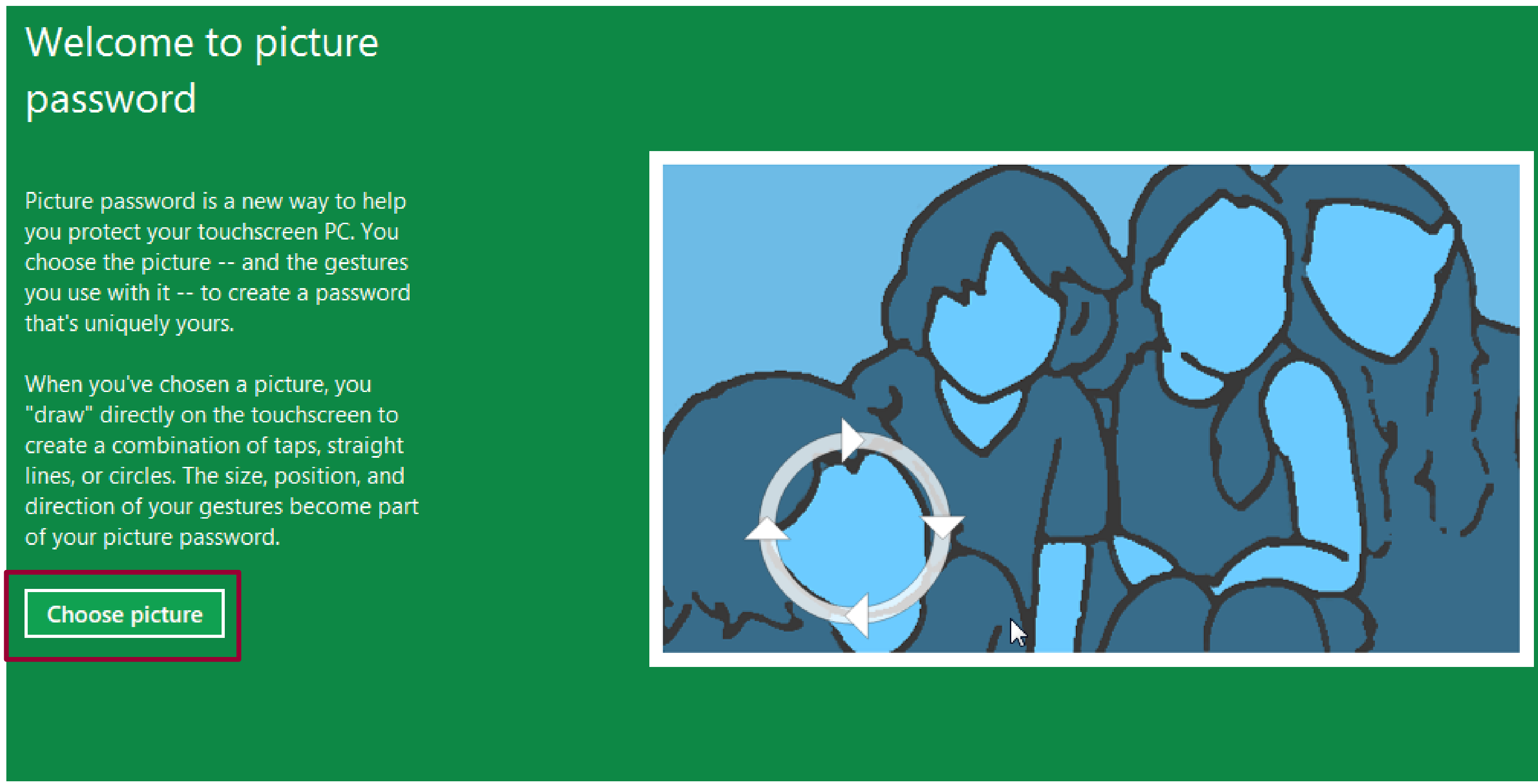
When you've chosen a picture, you "draw" directly on the touchscreen to create a combination of taps, straight lines, or circles. The size, position, and direction of your gestures become part of your picture password.

Choose picture



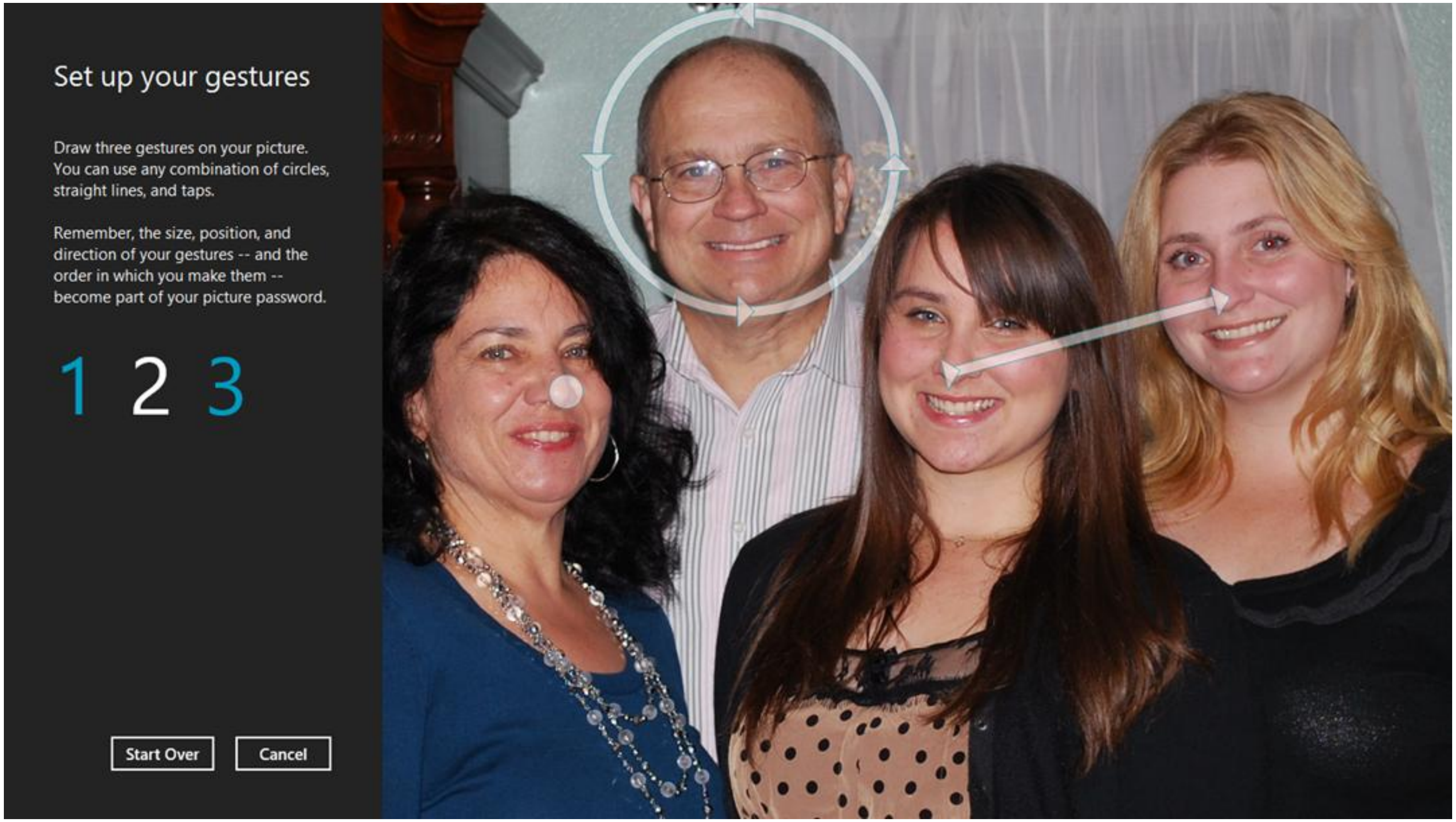
How PGA Works

- Autonomous picture selection by users



How PGA Works

- Three types of gestures are allowed
  - Tap
  - Circle
  - Line



Research Questions

1. How to understand user-choice patterns in PGA?
   - Background Pictures
   - Gesture Location
   - Gesture Type
   - Gesture Order

2. How to use these patterns to guess PGA password?

Outline

Part 1: Analysis of more than 10,000 PGA passwords collected from user studies

Part 2: A fully automated attack framework on PGA

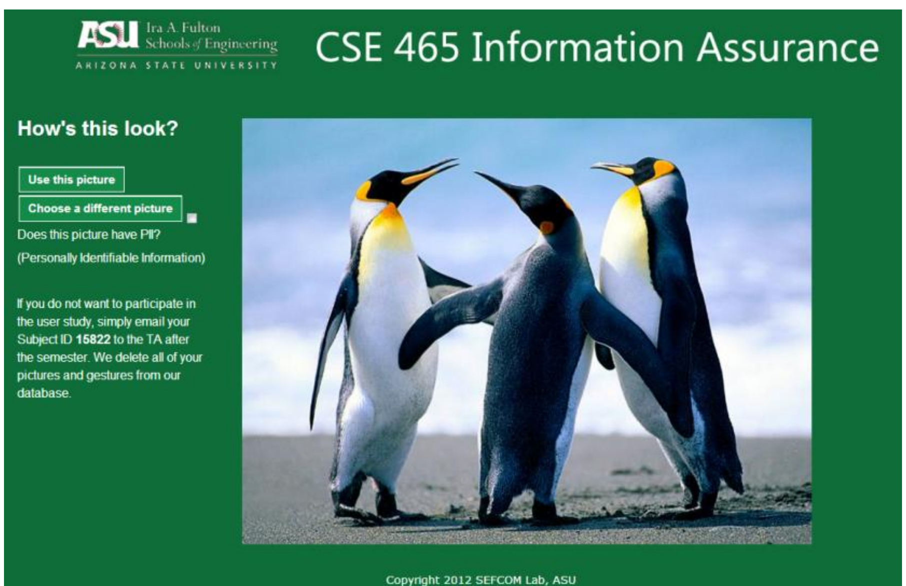
Part 3: Attack results on collected passwords

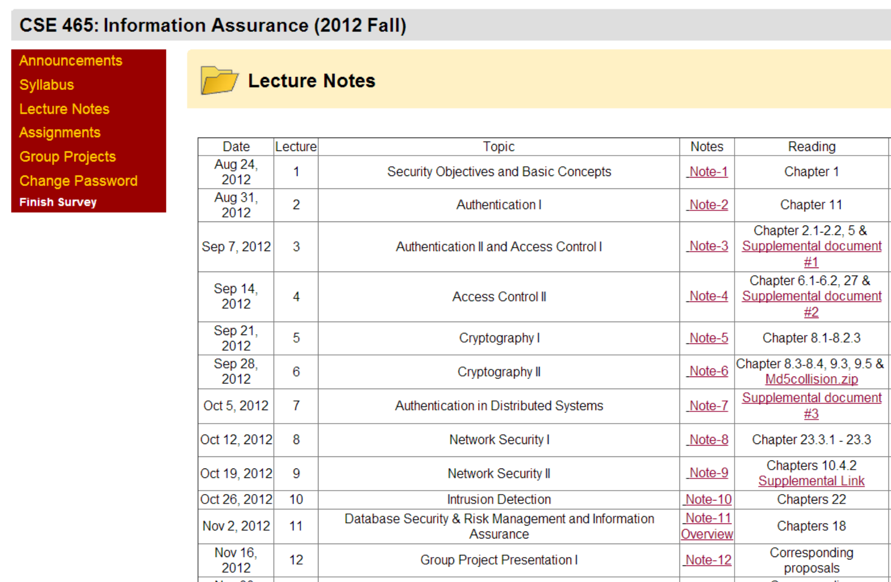
Part 1: User Studies

1. Web-based PGA system
   - Similarity to Windows PGA
     - Workflow
     - Appearance
2. Data collection
3. Analysis: survey and results

Part 1: User Studies

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





CSE 465: Information Assurance (2012 Fall)

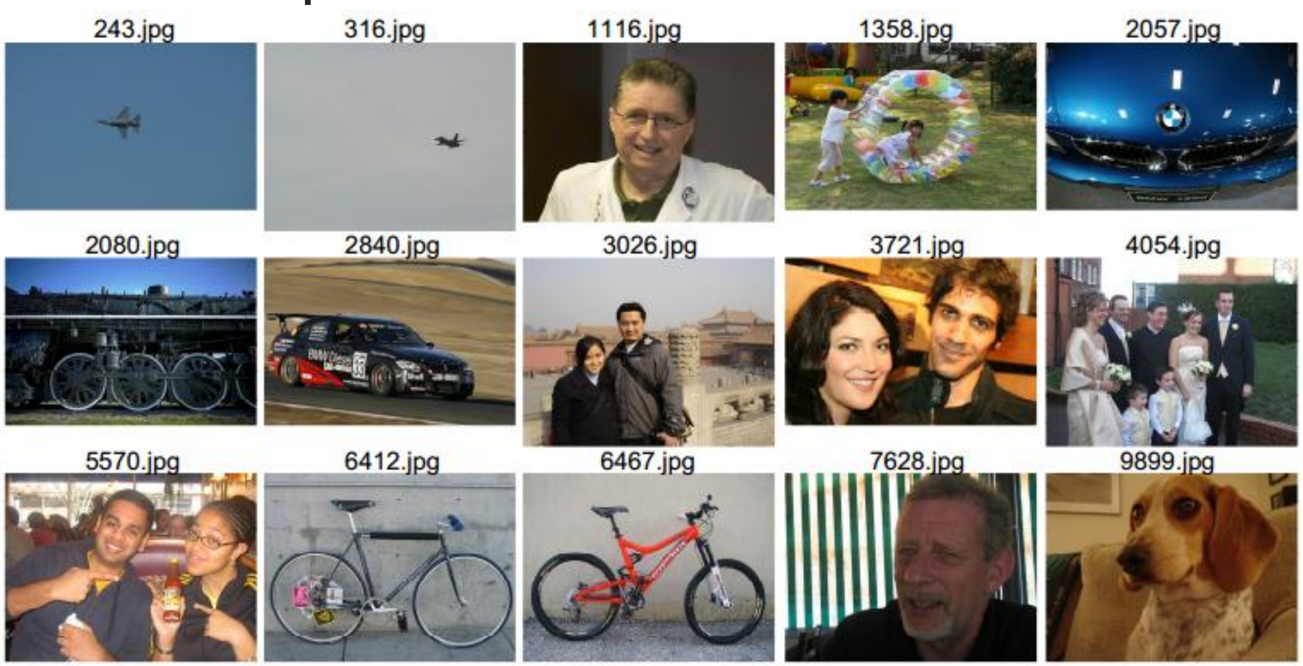
Announcements
Syllabus
Lecture Notes
Assignments
Group Projects
Change Password
Finish Survey

Lecture Notes

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 & Md5collision.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	1
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

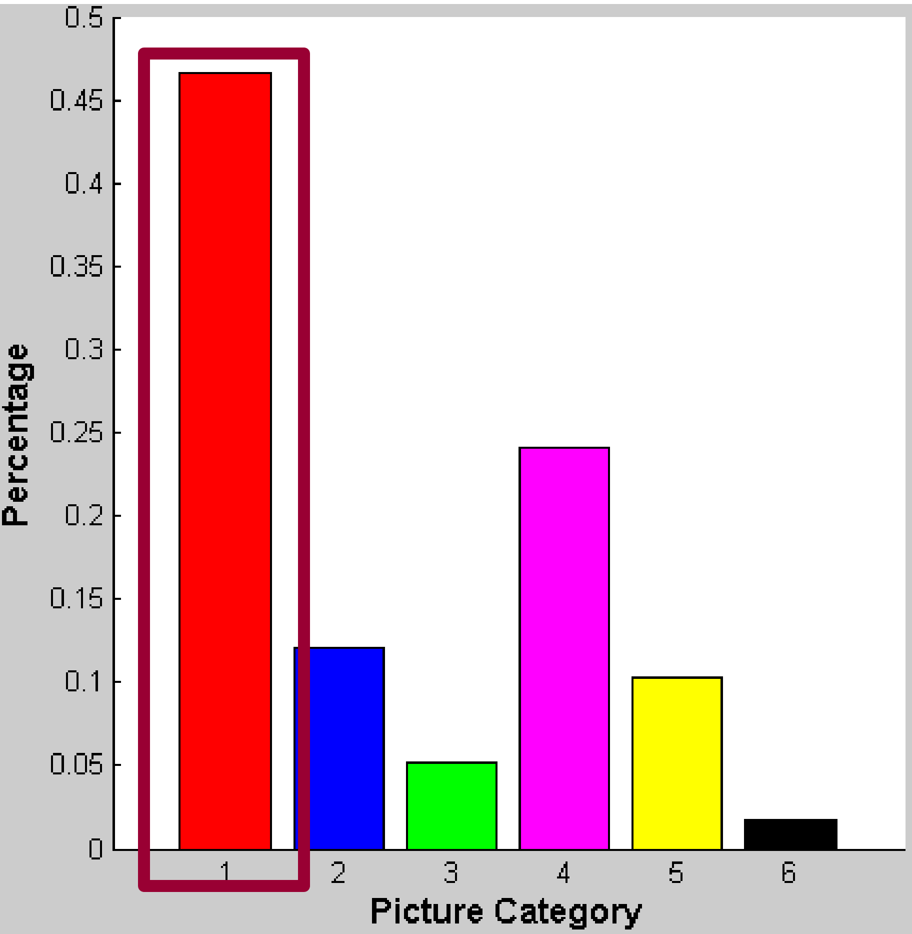
- Survey questions
  - General information of the subject
  - General feeling towards PGA
  - How she/he selects a background picture
  - How she/he selects a password

Part 1: User-choice Patterns

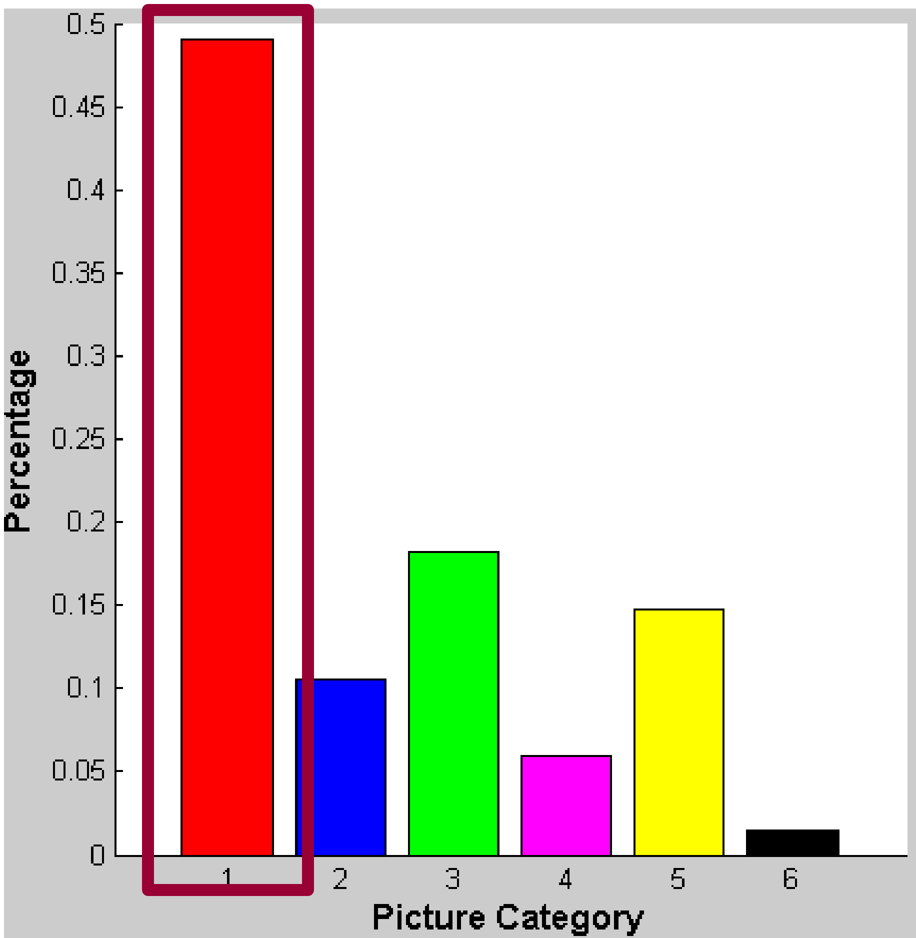
Background Picture

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

Dataset-1



Dataset-2 Survey



Part 1: User-choice Patterns

Why or why not picture of people

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

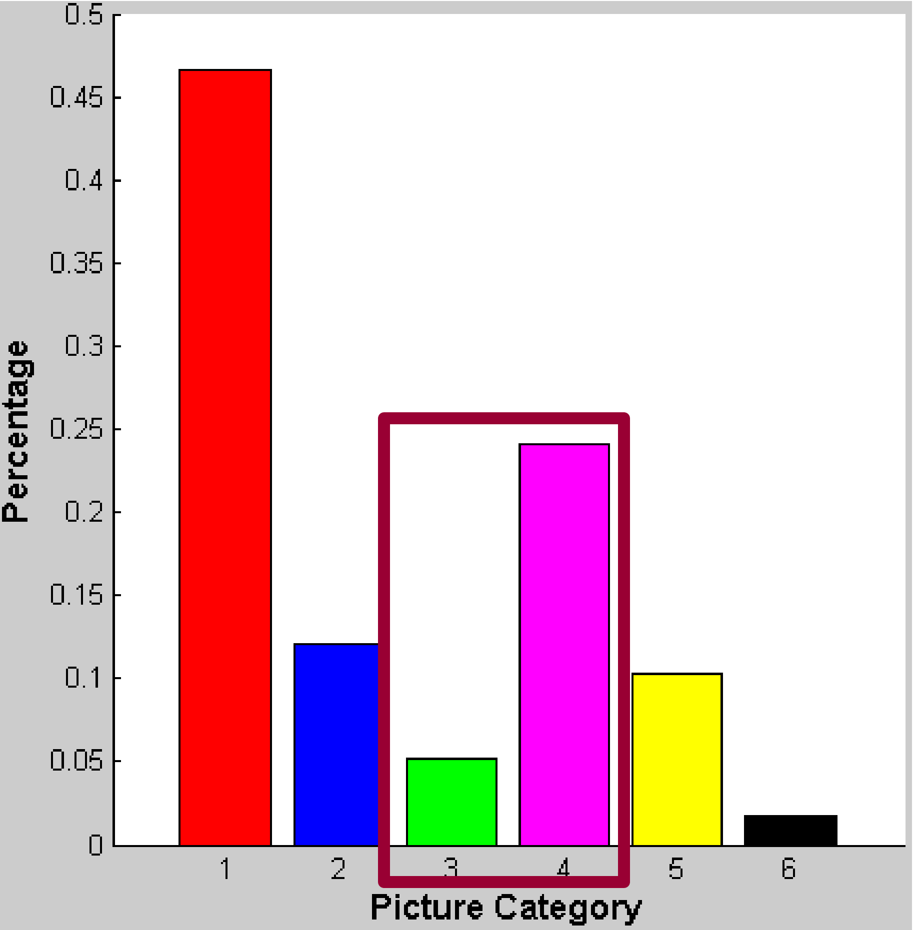
- Others:
  i) leak his or her identify or privacy
  'revealing myself or my family to anyone who picks up the device'

Part 1: User-choice Patterns

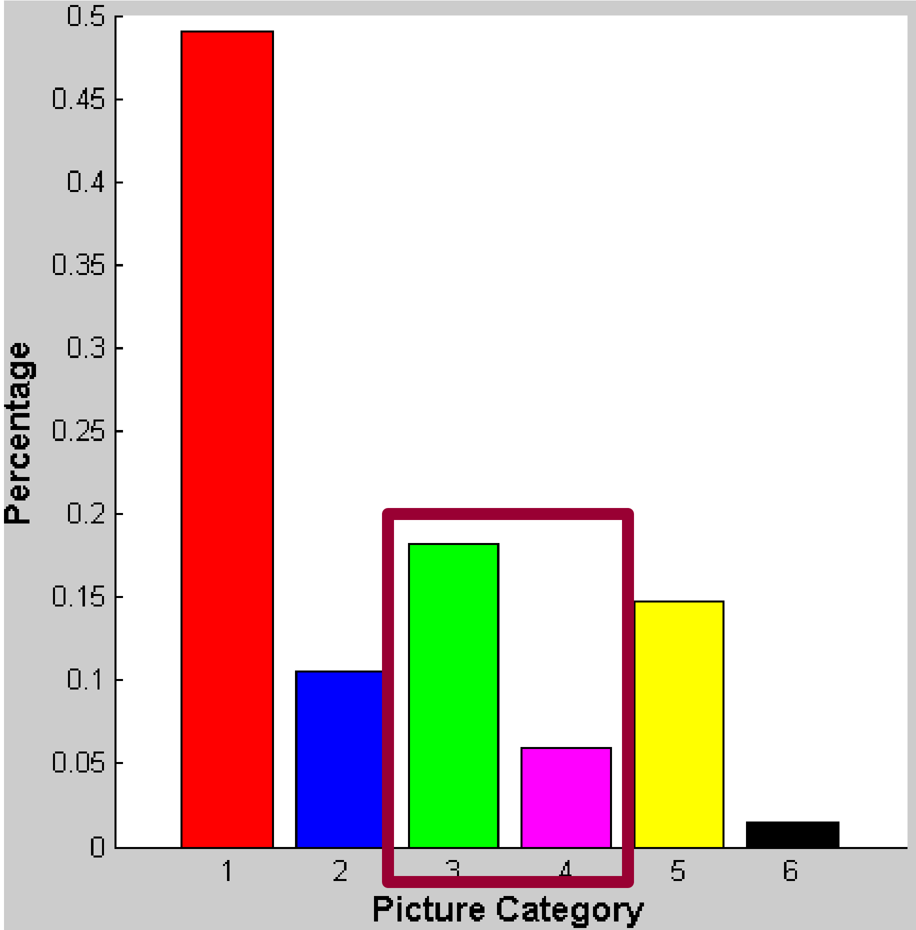
Background Picture

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

Dataset-1



Dataset-2 Survey



Part 1: User-choice Patterns

Why computer-generated pictures

- Dataset-1 population characteristics:
  - 81.8% Male
  - 63.6% Age 18-24, 24.0% Age 25-34
  - 100% College students

- Survey answers:
  - '*computer game is something I am interested [in] it*'
  - '*computer games picture is personalized to my interests and enjoyable to look at*'

Part 1: User-choice Patterns

Why computer-generated pictures

- Dataset-1 population characteristics:
    - 81.8% Male
    - 63.6% Age 18-24, 24.0% Age 25-34

The background picture tells much about the user's identity, personality and interests.

- Survey answers:
    - ‘*computer game is something I am interested [in] it*’
    - ‘*computer games picture is personalized to my interests and enjoyable to look at*’

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 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 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 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 gestures?

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

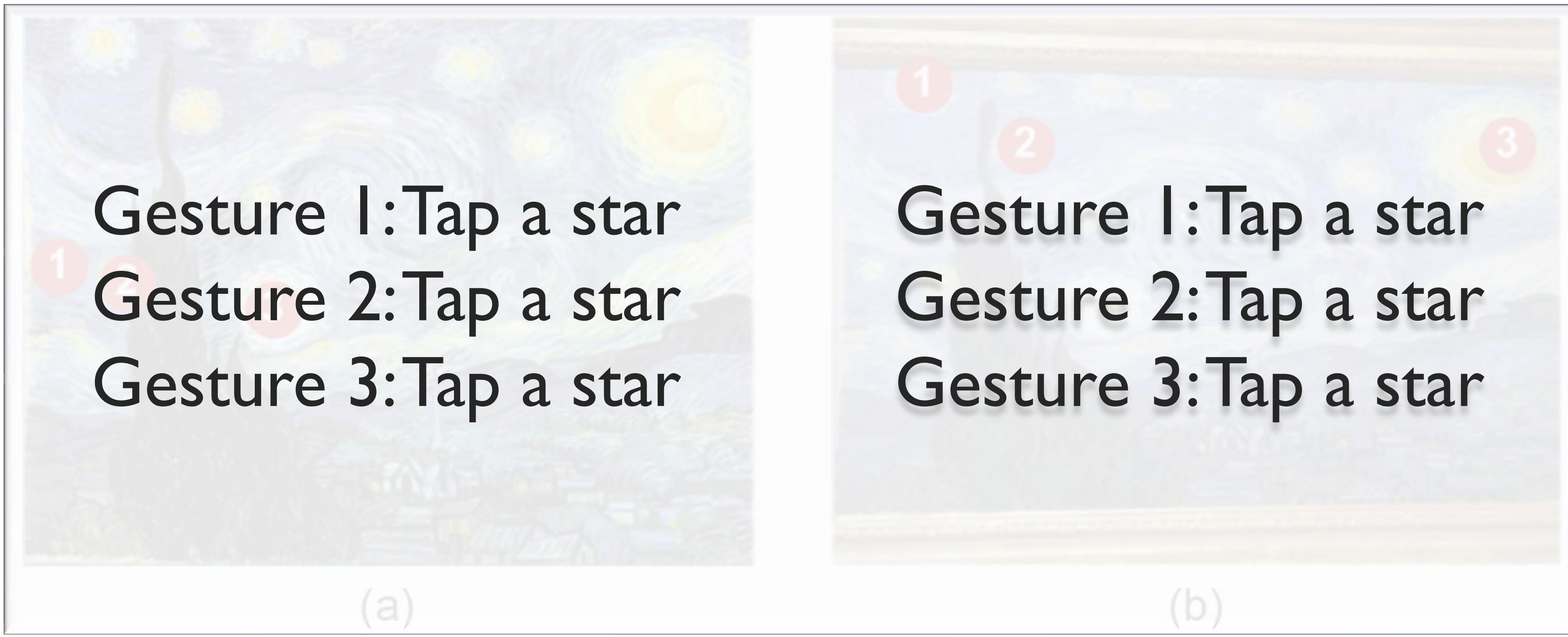
(a)

(b)

Part 1: User-choice Patterns

Gesture Locations (Civilization)

- Dataset-1
  - Two versions of *Starry Night* uploaded by two participants



(a) (b)

Gesture 1: Tap a star
Gesture 2: Tap a star
Gesture 3: Tap a star

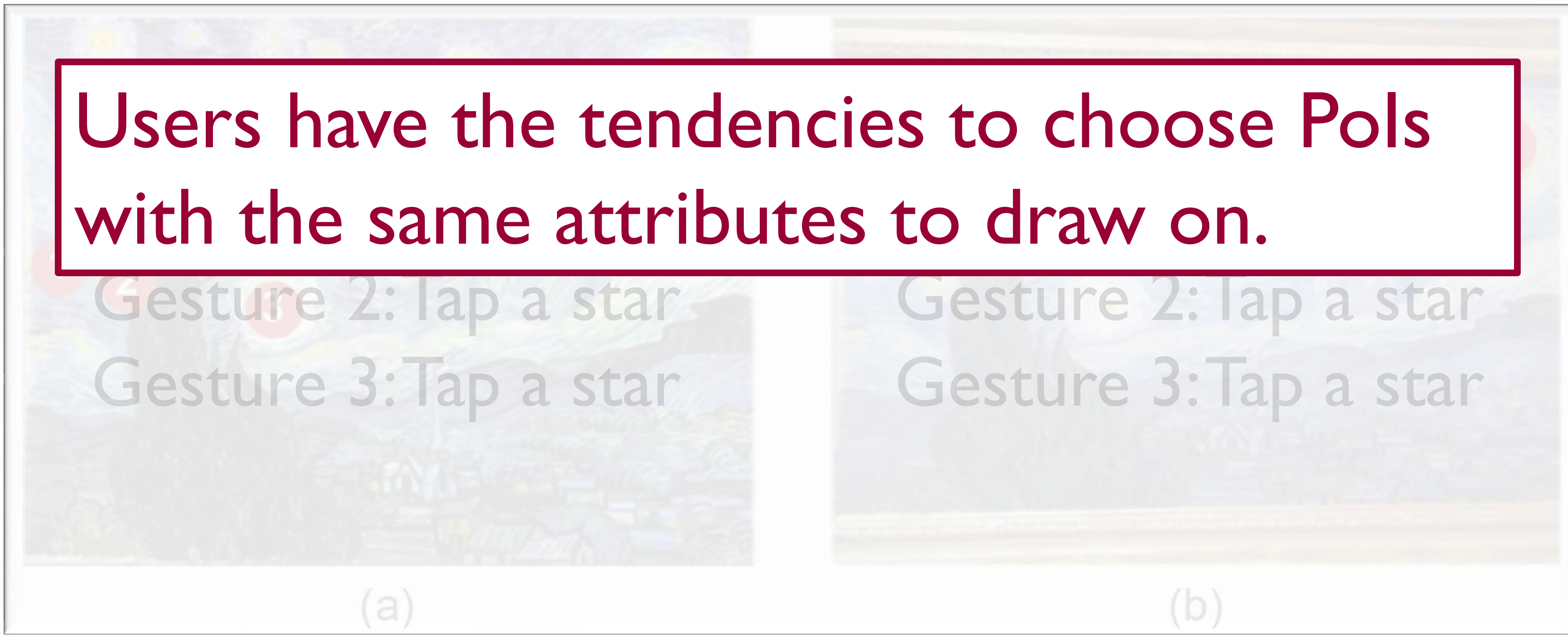
Gesture 1: Tap a star
Gesture 2: Tap a star
Gesture 3: Tap a star

Part 1: User-choice Patterns

Gesture Locations (Civilization)

- Dataset-1
  - Two versions of *Starry Night* uploaded by two participants

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



Part 1: User-choice Patterns

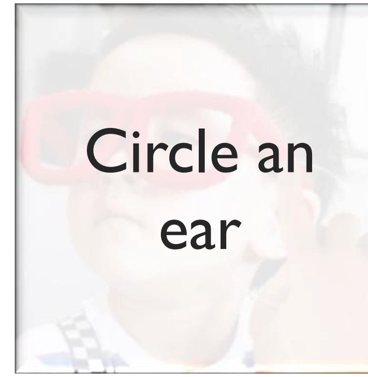
Windows PGA Advertisements

Asia

Part 1: User-choice Patterns

Windows PGA Advertisements

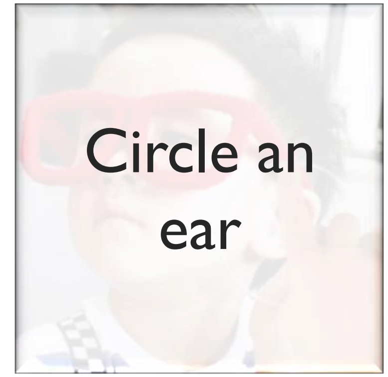
Asia



Part 1: User-choice Patterns

Windows PGA Advertisements

Asia

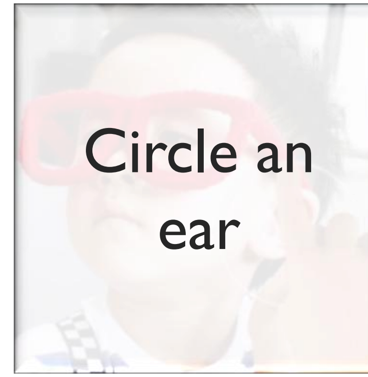


South America

Part 1: User-choice Patterns

Windows PGA Advertisements

Asia

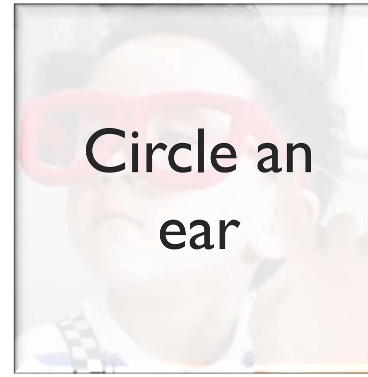


South America

Part 1: User-choice Patterns

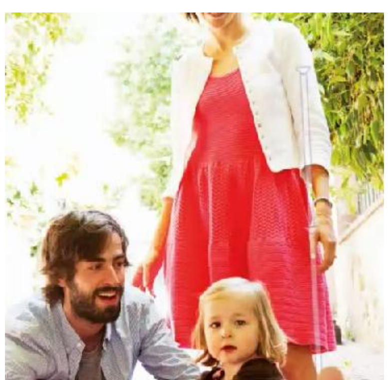
Windows PGA Advertisements

Asia



South America

Europe



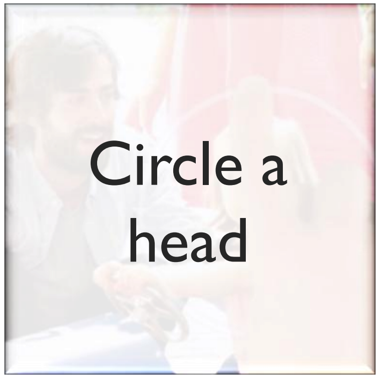
Part 1: User-choice Patterns

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

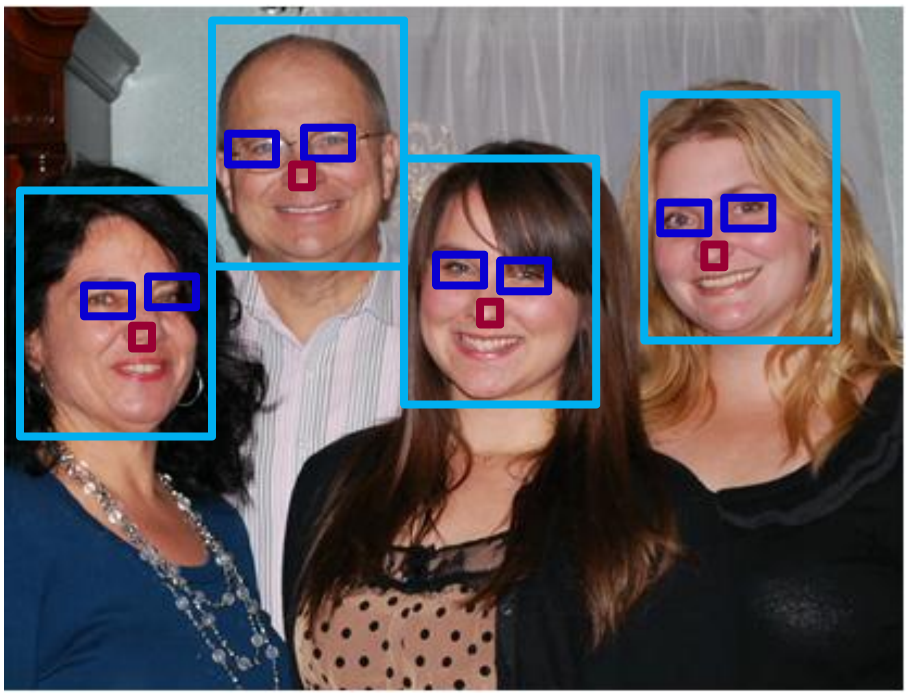
s(tap, nose)
Tap a nose in the picture

Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest

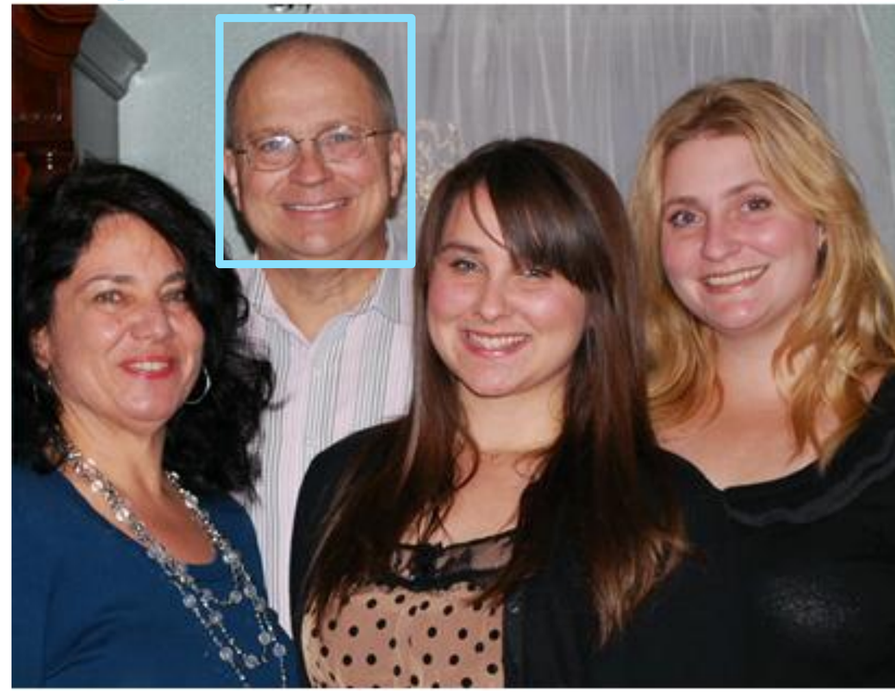


Part 2: Attack Framework

Extract Selection Functions

circle Password

face Points-of-Interest

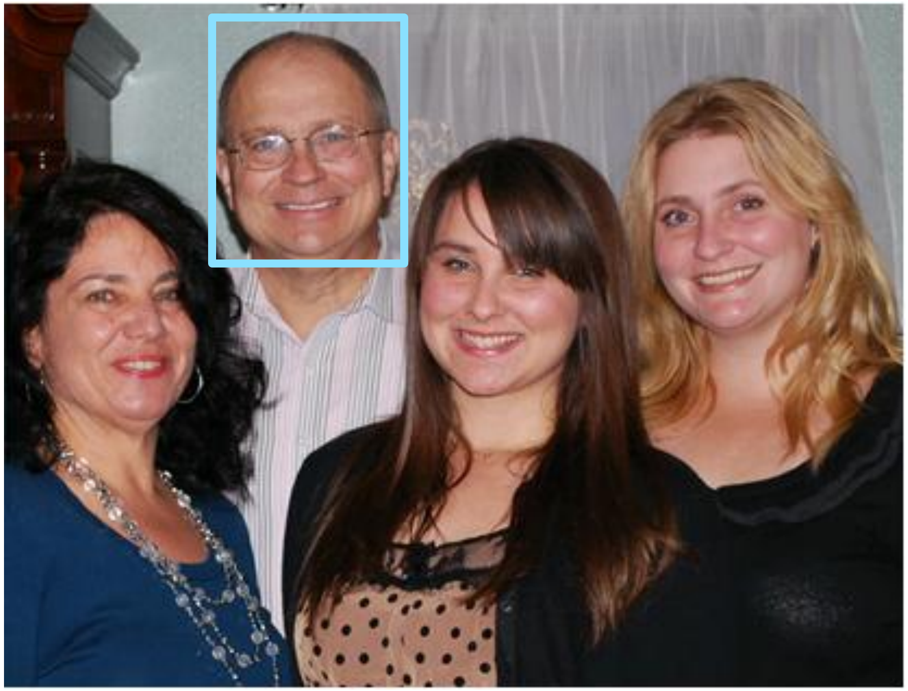


Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest



Function 1: *s(circle ,face)*

Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest

Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest

Function 2: *s(line, nose, nose)*

Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest

Part 2: Attack Framework

Extract Selection Functions

Password

Points-of-Interest

Function 3: *s(tap, nose)*

Part 2: Attack Framework

Apply Selection Functions

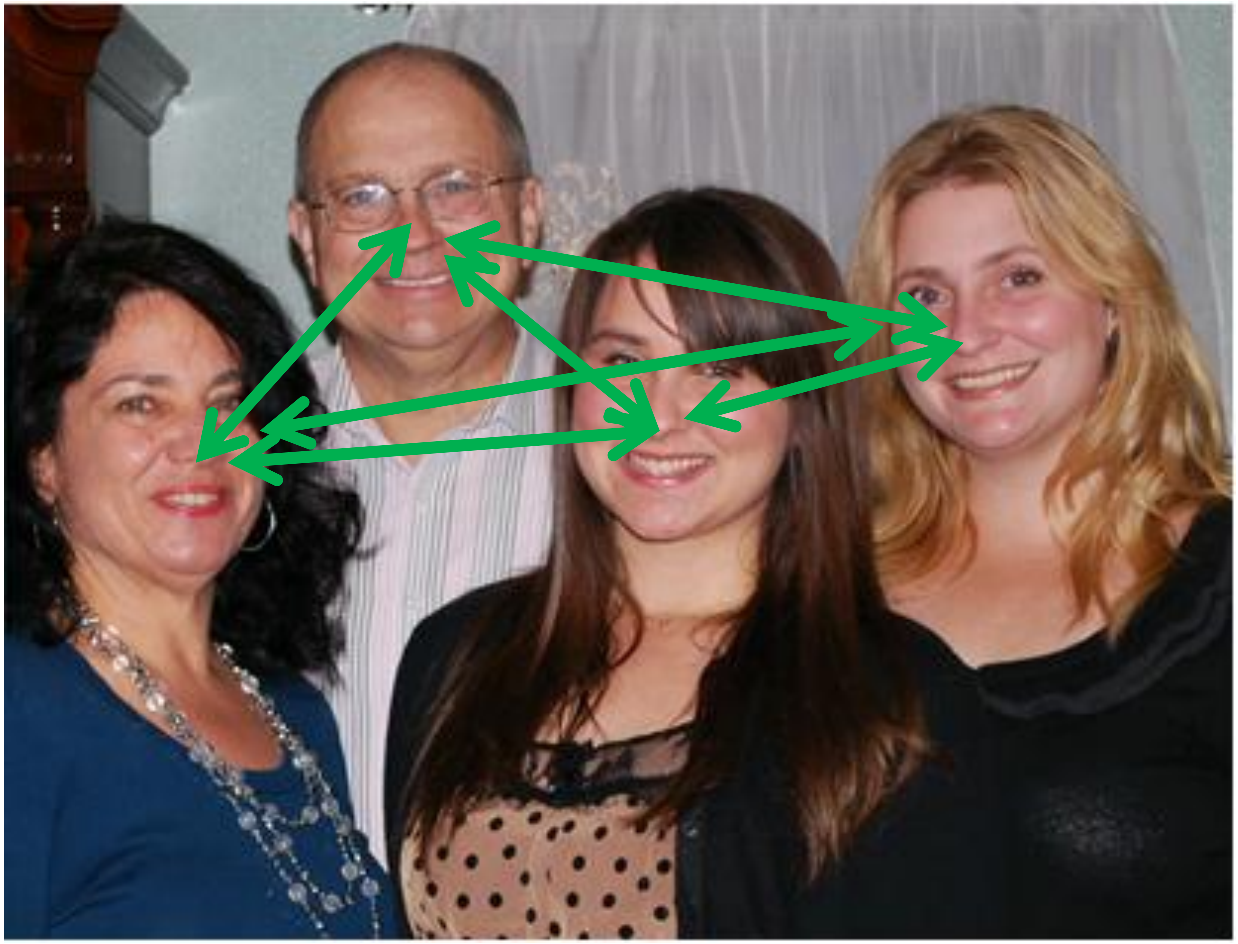
Function 1:

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

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: $4 \times 12 \times 4 = 192$

Part 2: Attack Framework

Rank Selection Functions

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

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

Part 3: Attack Results

Automatically Identify PoIs

- OpenCV as the computer vision framework
  - Object detection
    - Face, eye, nose, mouth, ear, body
  - Low-level feature detection
    - Circle
    - Color
  - Objectness measure: Alexe et al. (TPAMI'12)
    - Other standout regions

Part 3: Attack Results

Points-of-Interest Sets

$P^1_{A\text{-}40}$
- PoIs of Dataset-1
- Identified by OpenCV
- 40 PoIs at most

$P^2_{A\text{-}40}$
- PoIs of Dataset-2
- Identified by OpenCV
- 40 PoIs at most

$P^2_{L\text{-}15}$
- PoIs of Dataset-2
- Manually labeled
- 15 PoIs at most

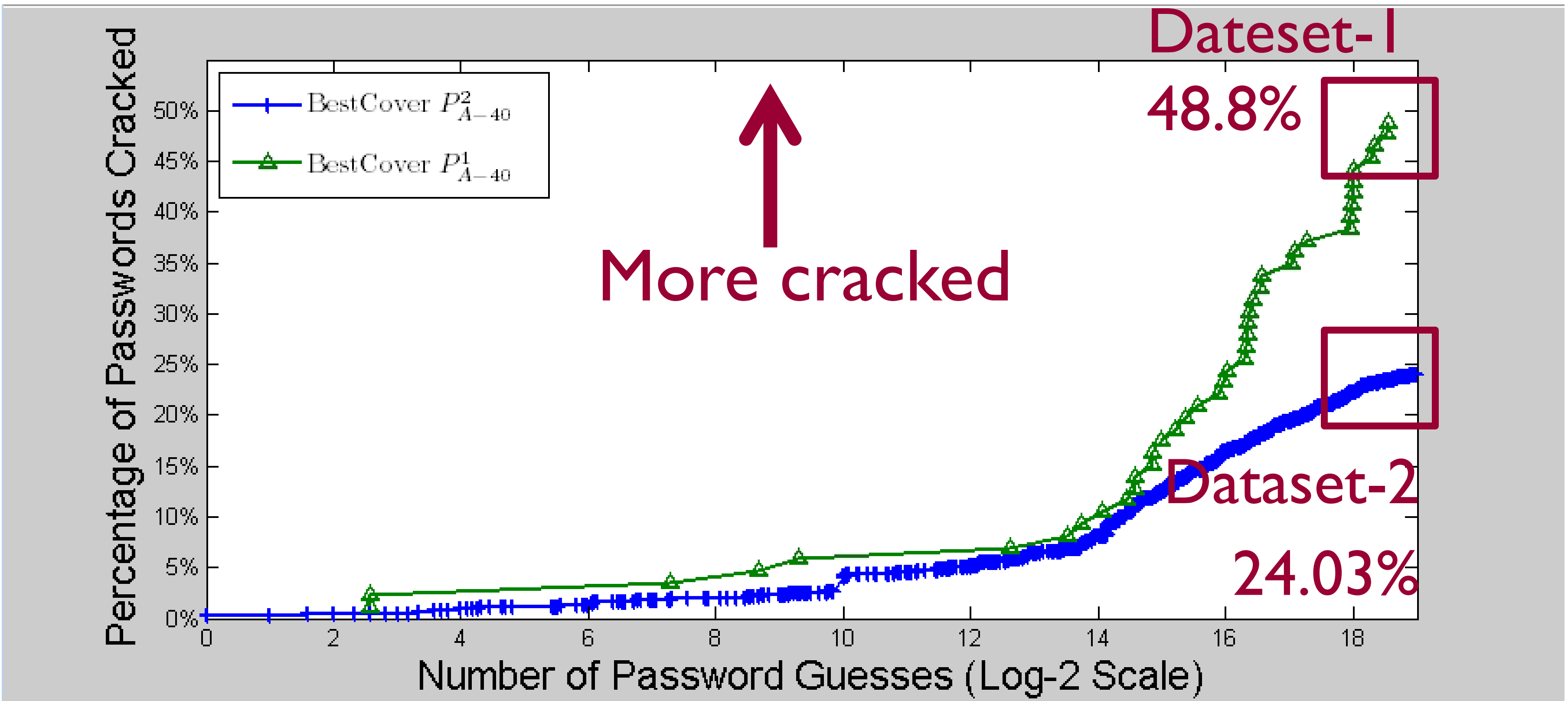
Part 3: Attack Results

Methodology

- Guessability on passwords of previously unseen pictures
- Dictionary size: $2^{19} = 524{,}288$

Part 3: Attack Results

Dateset-1 vs. Dateset-2

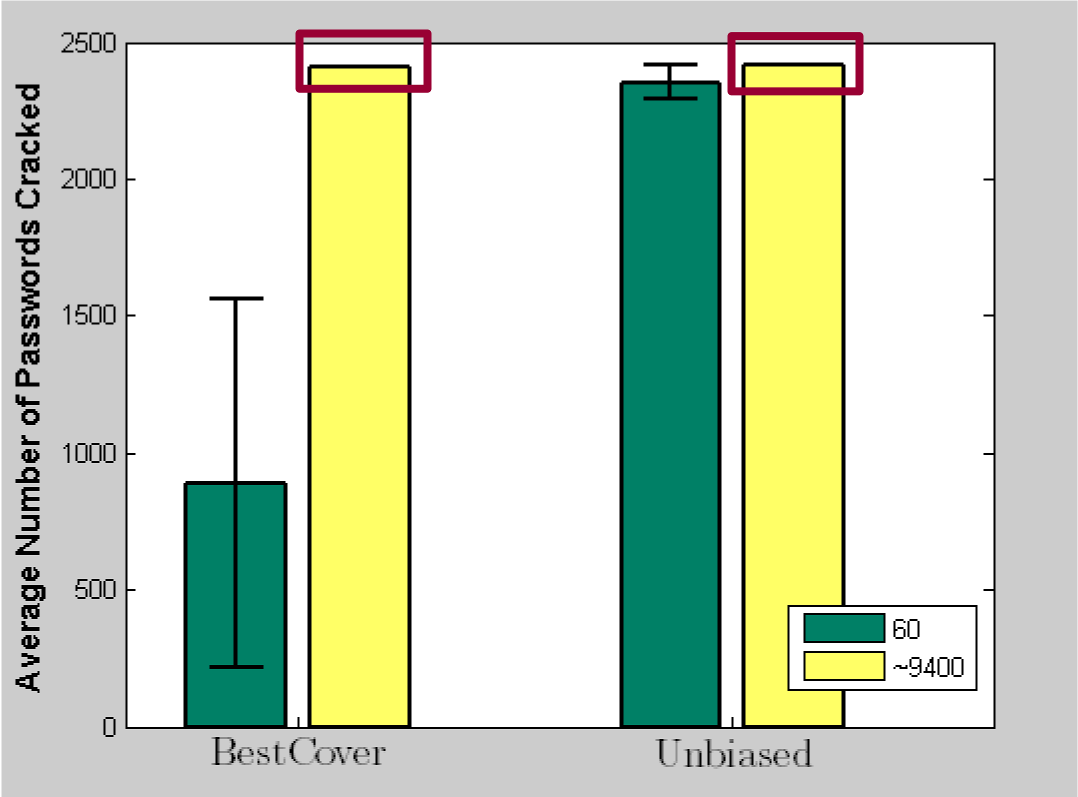


Part 3: Attack Results

BestCover vs. Unbiased

~9400 training passwords

BestCover 24.03% Unbiased 24.09%



Part 3: Attack Results

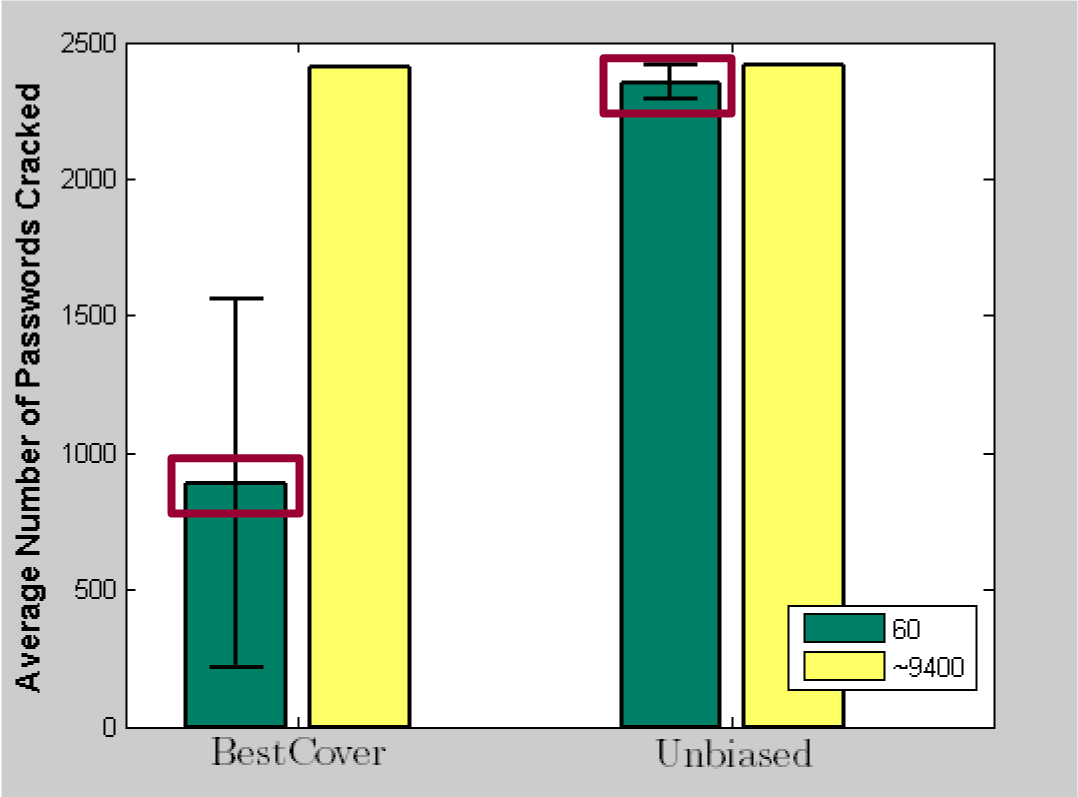
BestCover vs. Unbiased

60 training passwords

Unbiased 23.44%

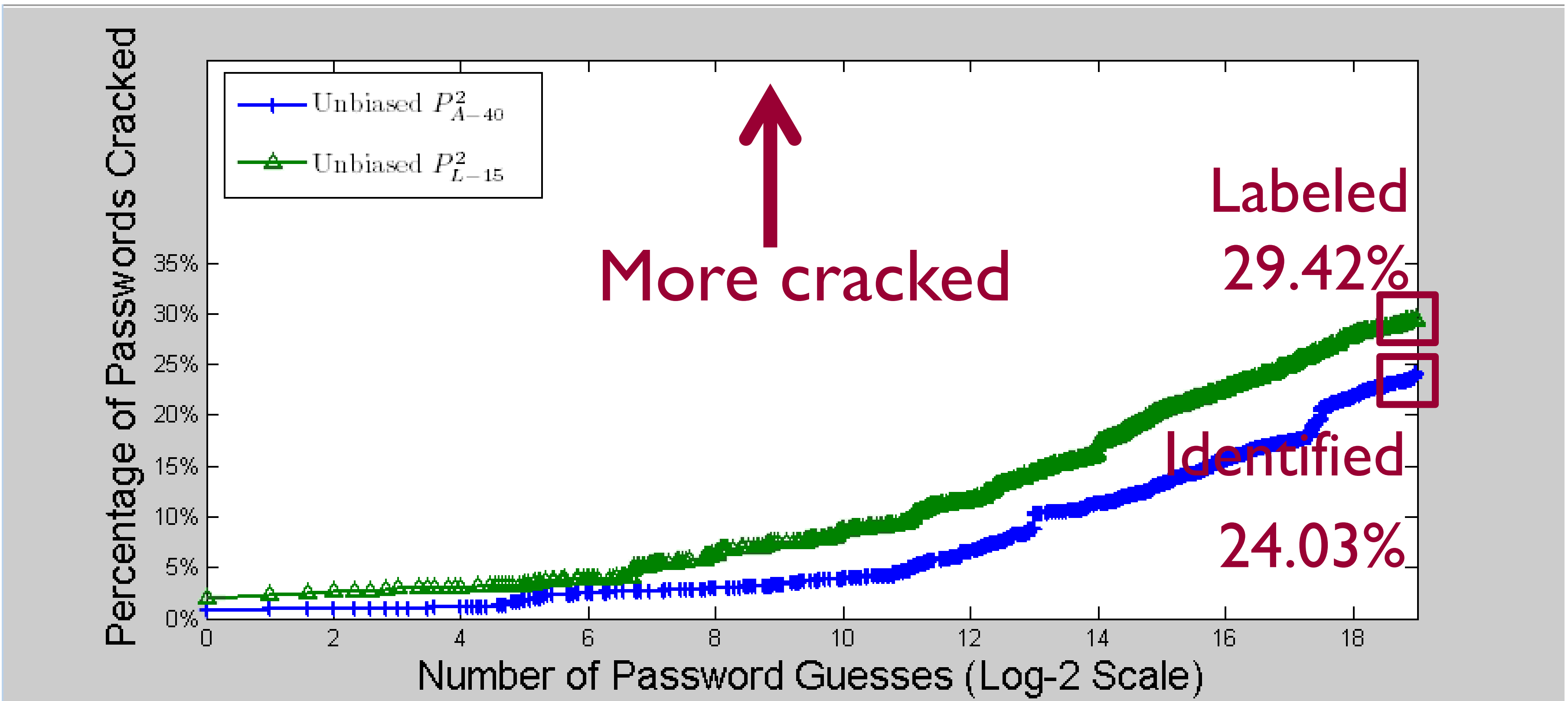
BestCover

13.27%



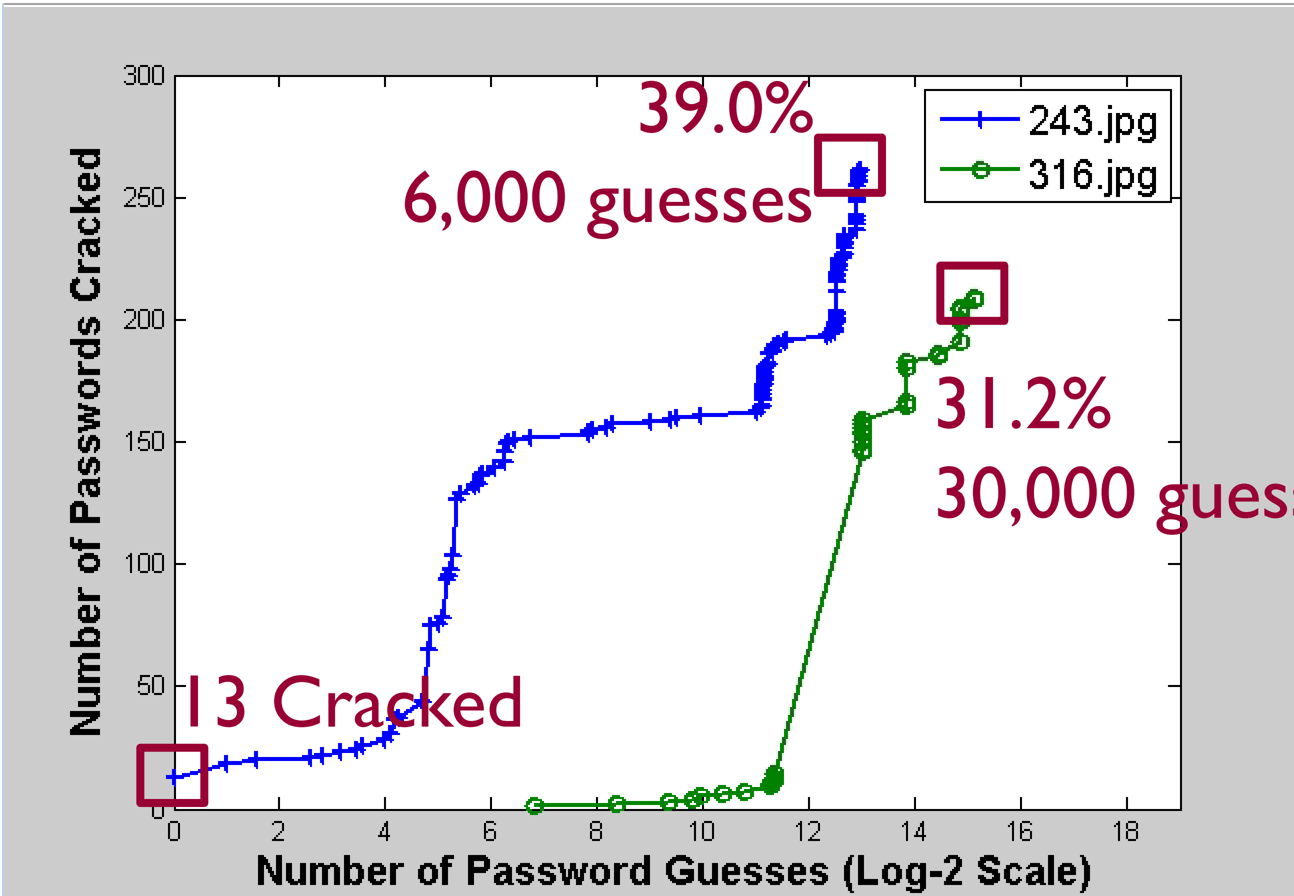
Part 3: Attack Results

Labeled PoI set vs. OpenCV-Identified PoI set



Part 3: Attack Results

Simple Pictures (Unbiased algorithm)

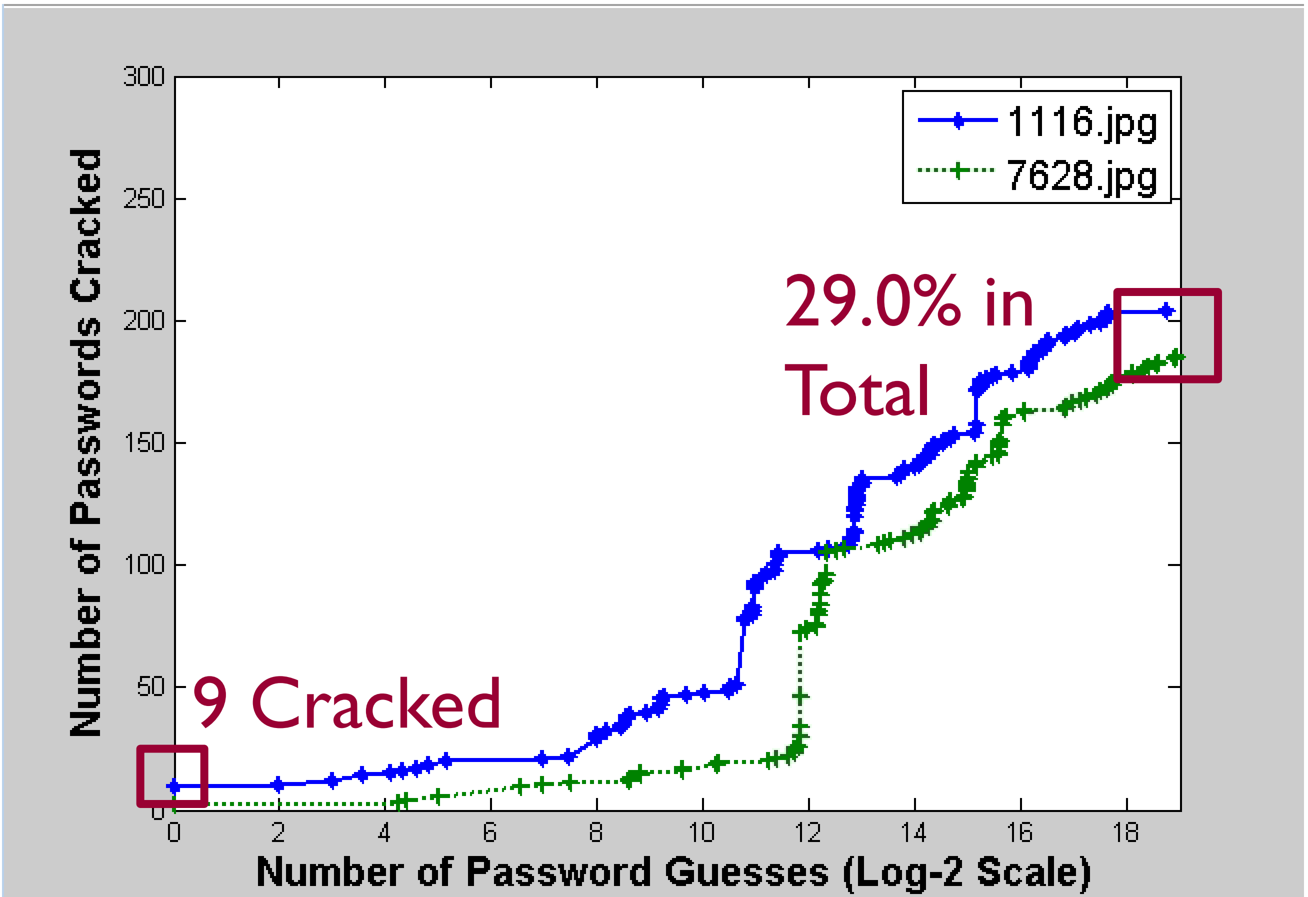


243.jpg

316.jpg

Part 3: Attack Results

Portraits (Unbiased algorithm)

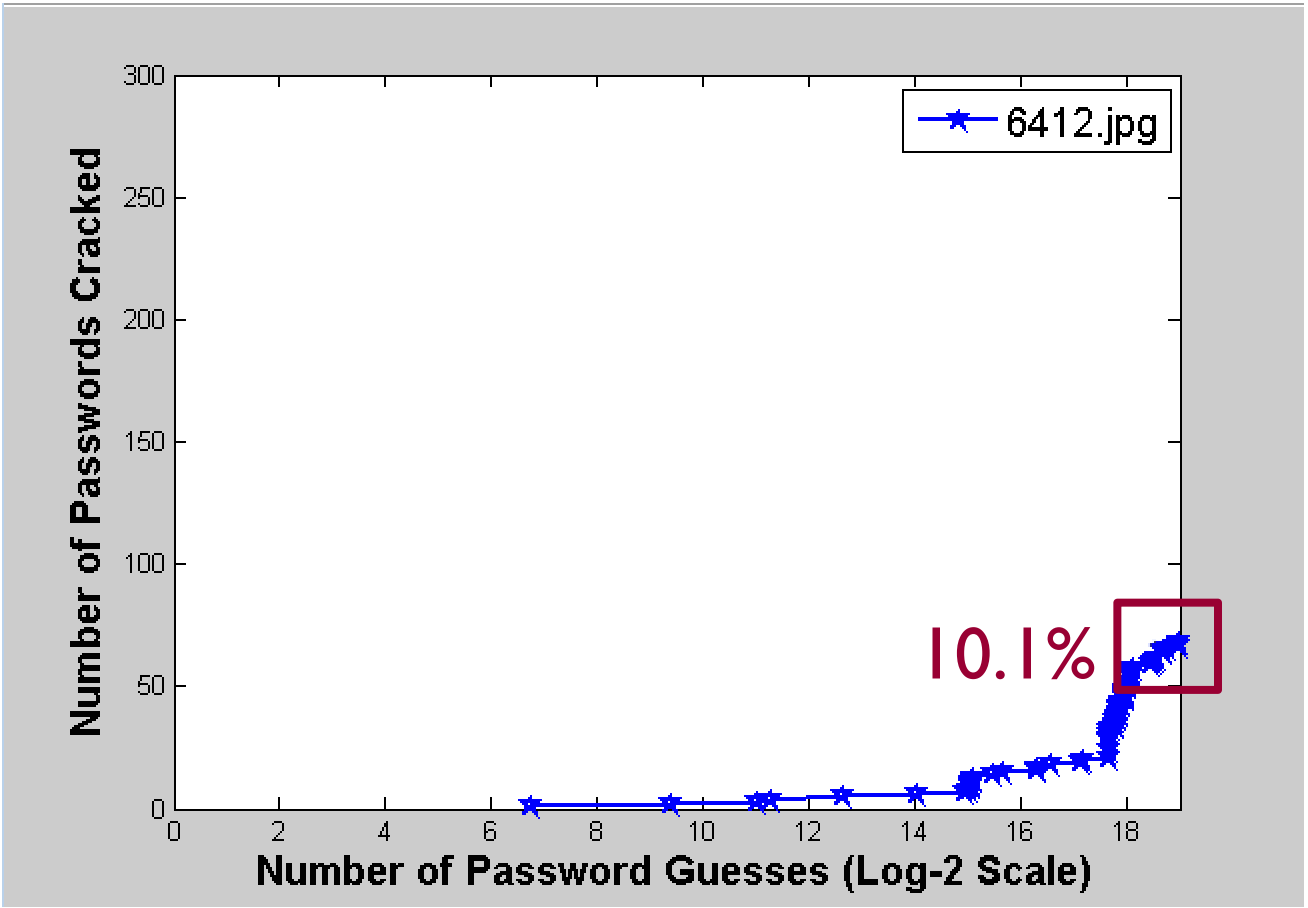


1116.jpg

7628.jpg

Part 3: Attack Results

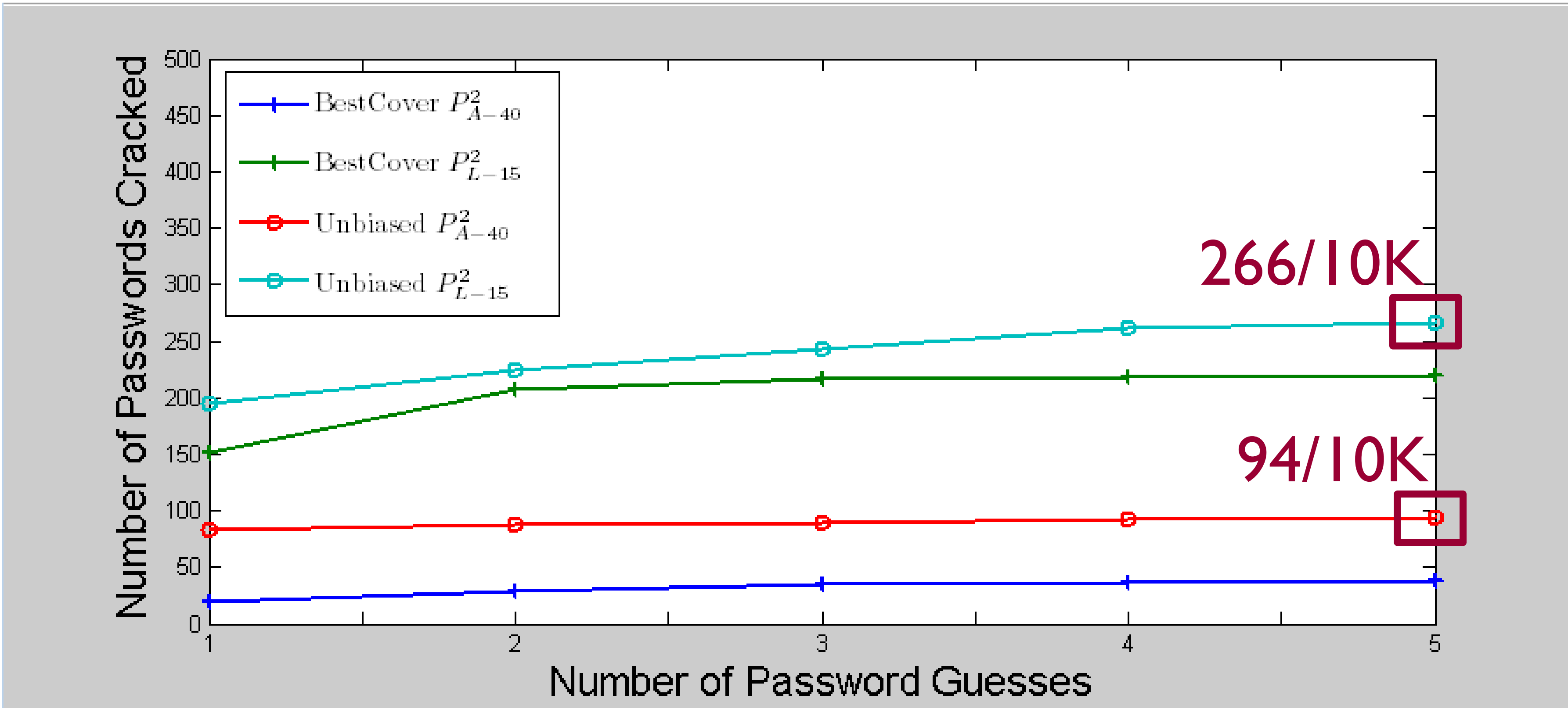
Complex Picture (Unbiased algorithm)



6412.jpg

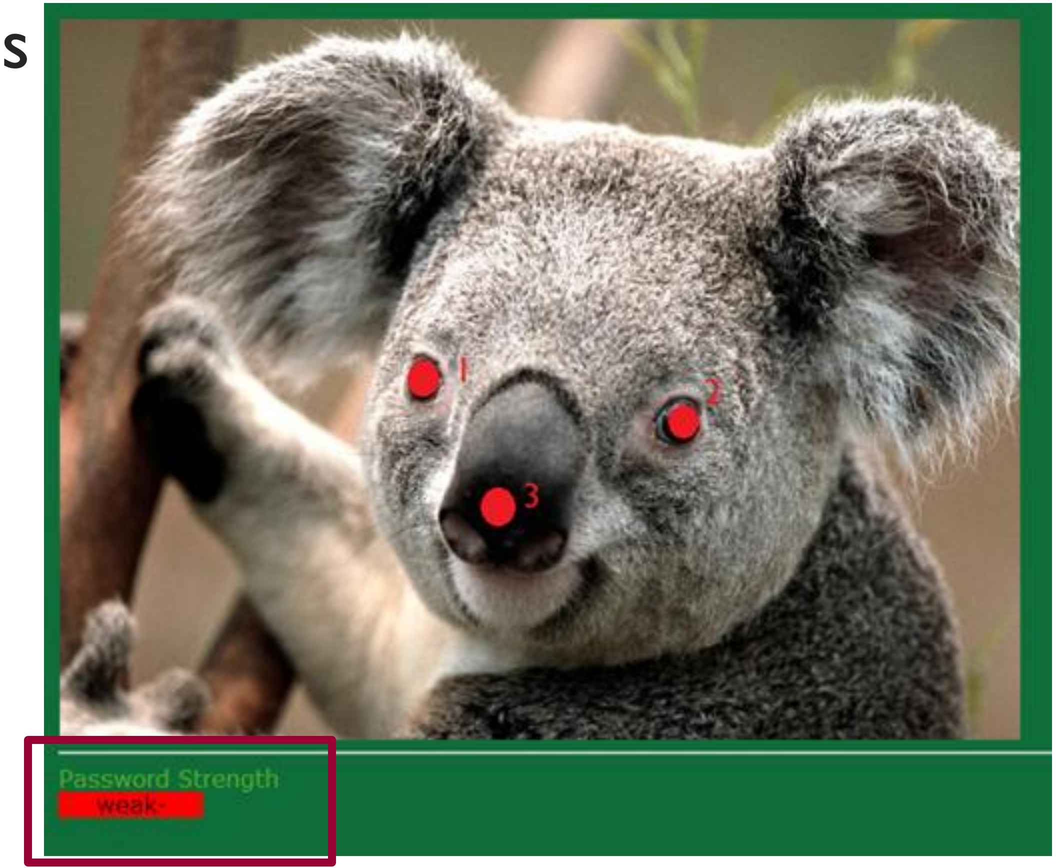
Part 3: Attack Results

Online Attacks on Dataset-2



PGA Password Strength Meter

- https://honeyproject1.fulton.asu.edu/stmidx
- BestCover algorithm
- Generate dictionary and calculate strength in 20 seconds



Summary and Future Work

- We have presented an analysis of user-choice patterns in PGA passwords
- We have proposed an attack framework on PGA
- We have evaluated our approach on collected datasets

- We plan to improve online attack results by integrating shoulder-surfing and smudge attacks into our framework

Thank you!
Q & A