POLITECNICO DI MILANO

DEEPSEC





Social Authentication:
Vulnerabilities, Mitigations, and Redesign

Marco Lancini

DEEPSEC 2014
November 21

About

- **2013 – M.Sc. in Engineering of Computing Systems @** POLITECNICO DI MILANO
  - Computer Security Group
  - This talk is based on my M.Sc. Thesis
- **2013 – Researcher @** CEFRIEL FORGING INNOVATION POLITECNICO DI MILANO
  - Security Research
  - Vulnerability Assessment & Penetration Testing
  - Web Applications & Mobile Security
- **@lancinimarco**

Online Social Networks

- **Huge user base**
- **Massive amount of personal information**
- **Widespread adoption of single sign-on services**

- **Appealing targets for online crime**
  - Identity theft
  - Spamming
  - Phishing
  - ~~Selling stolen credit cards numbers~~ → Selling compromised accounts

- **97% of malicious accounts are compromised, not fake**

Keeping Stolen Accounts Safe

- **TWO-FACTOR AUTHENTICATION**
  - *Knowledge* factor: "something the user *KNOWS*" (password)
  - *Possession* factor: "something the user *HAS*" (hardware token)

- Adopted by high-value services (online banking, Google services)

- **Pro**
  - Prevent adversaries from compromising accounts using stolen credentials
  - **The risk of an adversary acquiring both is very low**

- **Drawbacks (token)**
  - Inconvenient for users
  - Costly deploy

- **Drawbacks (SMS)**
  - Sent in plain text
  - Can be intercepted & forwarded
  - Phones easily lost and stolen

Social Authentication

- **Challenge = balance strong security with usability**

- **Social Authentication**
  - 2FA scheme that tests **the user's personal social knowledge**
    - only the intended user is likely to be able to answer

  - Using a "**social CAPTCHA**"
    - one or more challenge questions based on information available in the social network (user's activities and/or connections)

  - Eliminates the key issues of **traditional CAPTCHAs**
    - (at times) incredibly hard to decipher
    - vulnerable to human hackers
      (only meant to defend against attacks by computers)
      - "*CAPTCHA farming*"

FACEBOOK'S SOCIAL AUTHENTICATION

Social Authentication (SA)

- **Two-factor authentication scheme**
  - Tests the user's personal social knowledge
  - 2nd factor:

    ~~"something the user HAS" (hardware token)~~

    "something the user KNOWS" (**FRIEND**)

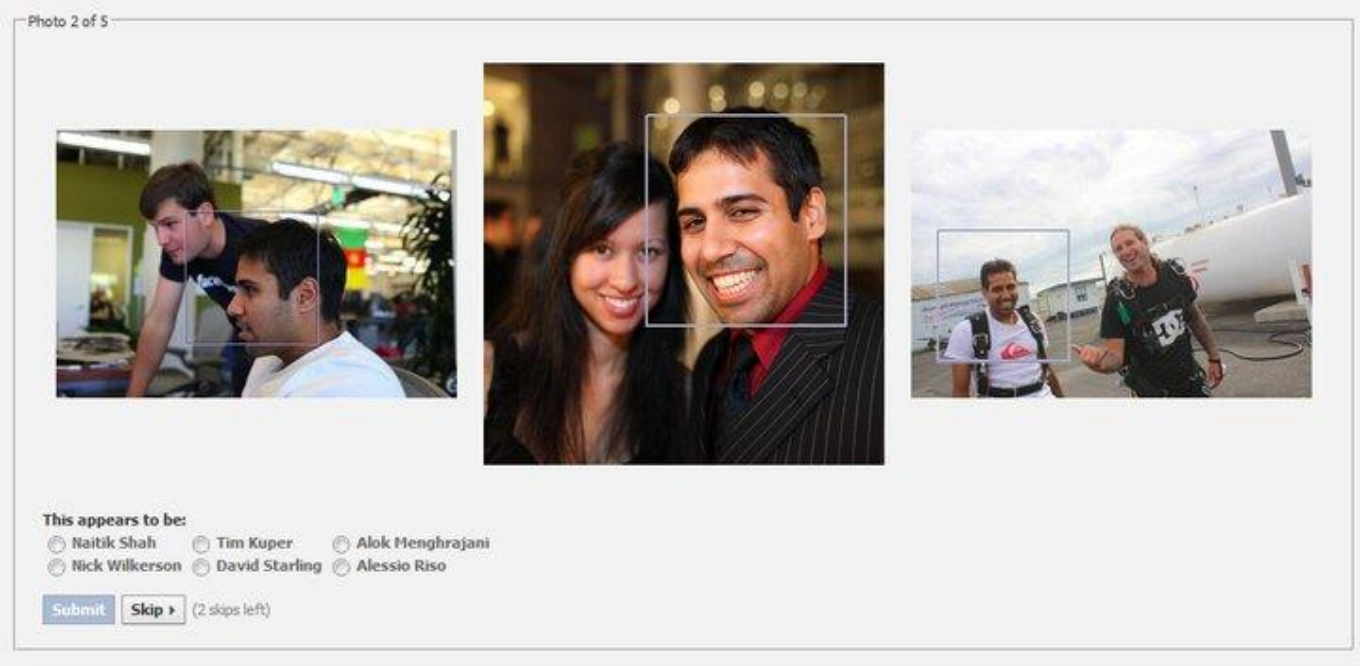
- **User's credentials authentic only if he can correctly identify his friends**

- **The user can recognize his friends whereas a stranger cannot**

  Attackers halfway across the world might know a user's password, but they don't know who his friends are

- **Triggering: When login considered suspicious**

How It Works



- **7 challenges**
- **Each challenge (page)**
  - 3 photos of a friend
  - 6 possible answers ("suggestions")

- User has to correctly answer **5 challenges** (2 errors/skips)
- Within the **5 minutes** time limit

Threat Model

- **Friend = anyone inside a user's online social circle**
  - Has access to information used by the SA mechanism

- **SA considered**
  - **Safe** against adversaries that
    - Have stolen credentials
    - Are strangers (not members of the victim's social circle)

  - **Not safe** against
    - Close friends
    - Family
    - Any tightly connected network (university)
      - Any member has enough information to solve the SA for any other user in the circle

VULNERABILITY ASSESSMENT OF SA

SA Photo Selection

"Are photos randomly selected?"

2,667 **photos from real SA tests**

- 84% containing faces in *manual inspection*
- 80% in automatic inspection by software

3,486 **random** Facebook photos
(from our dataset of 16M)

- 69% contained faces in *manual inspection*

- The baseline number of faces per photo is lower in general than in the photos found in SA tests
- **Face detection procedures used for selecting photos with faces**

Motivation

- **84% are photos with faces**

SA solvable by humans

- **80% are photos with faces that can be detected by face-detection software**

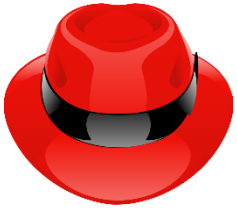
Can a <u>stranger</u> bypass SA in an automated manner?

- position himself inside the victim's social circle
- gaining the information **necessary** to defeat the SA

Attacker Models

CASUAL ATTACKER

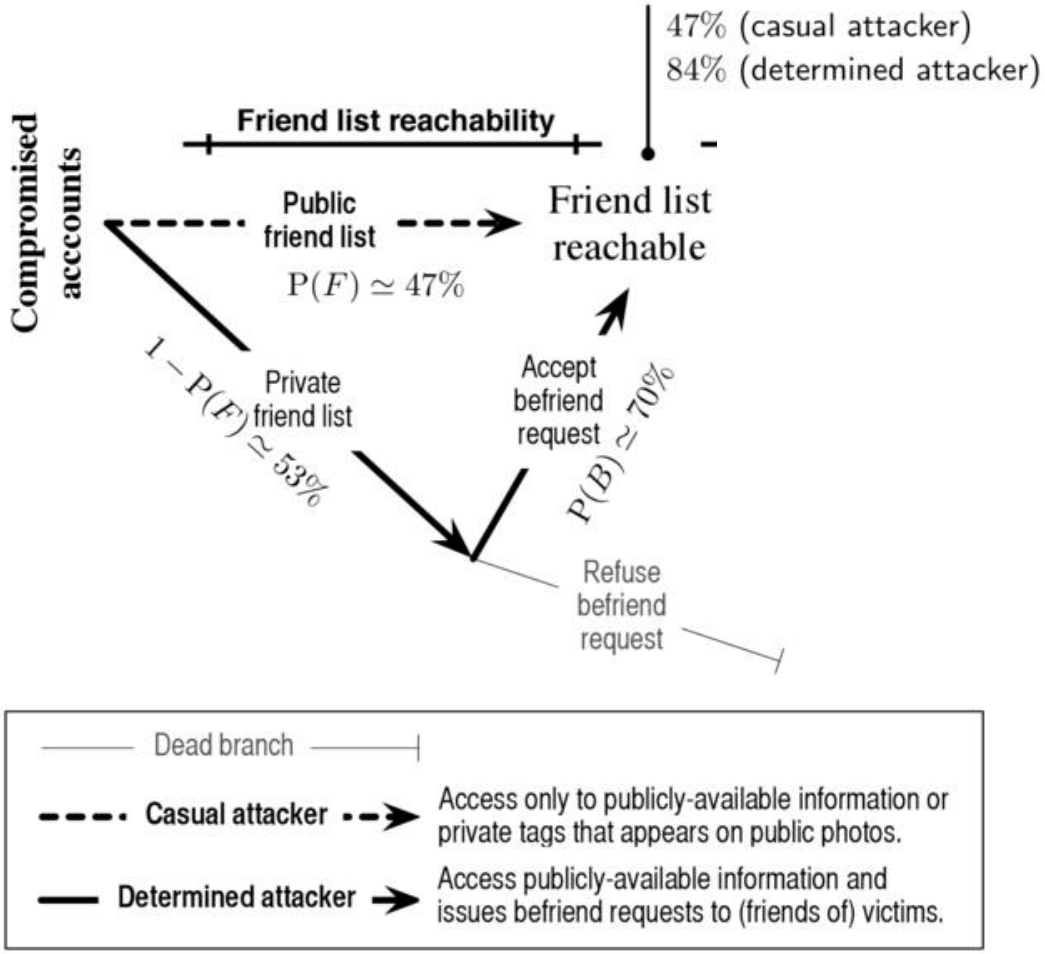
- Interested in compromising the **greatest possible number** of accounts
- Collects publicly available data
- May lack some information



DETERMINED ATTACKER

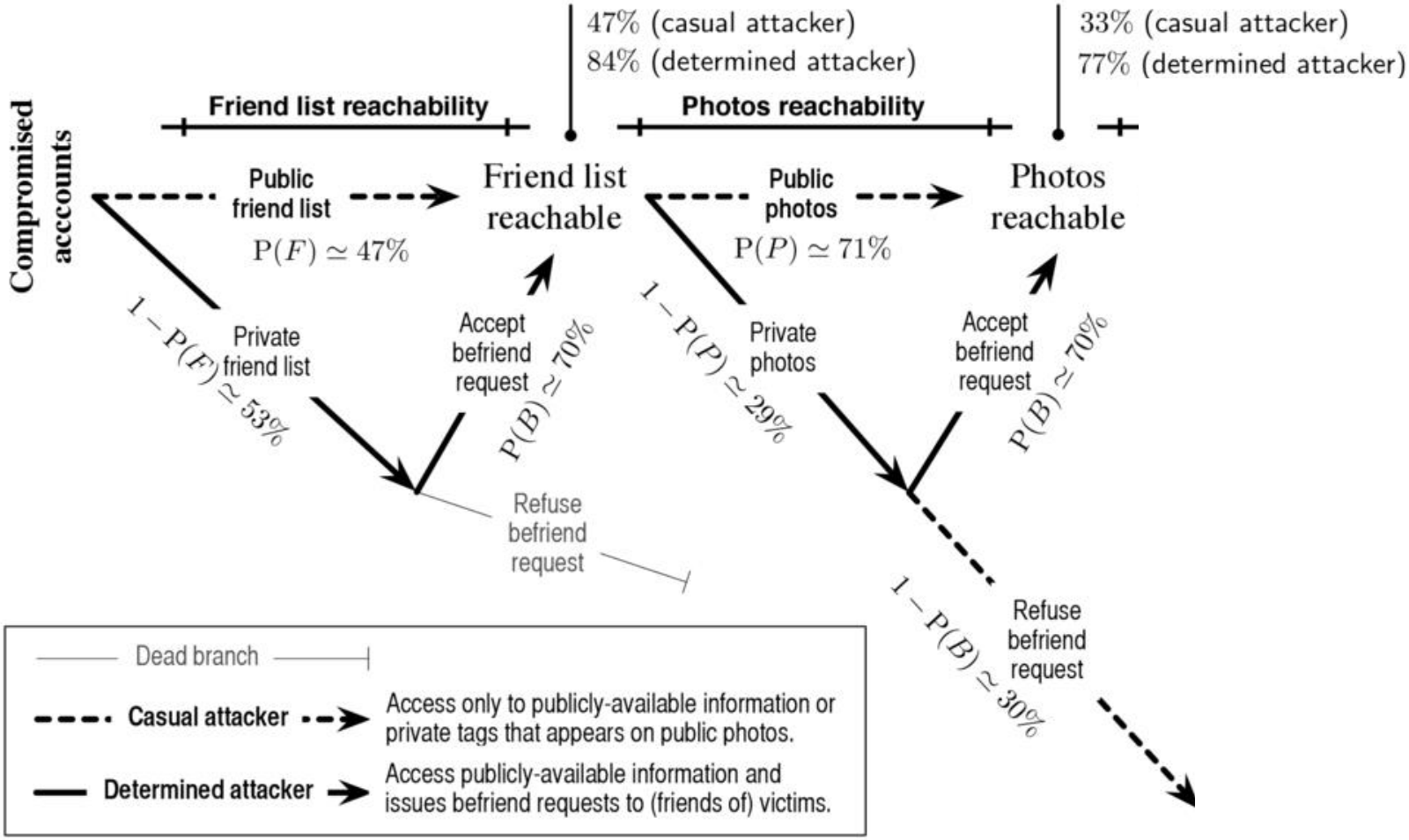
- Focused on a **particular target**
- Penetrates victim's social circle
- Collect as much private data as possible

Attack Surface Estimation – Friends



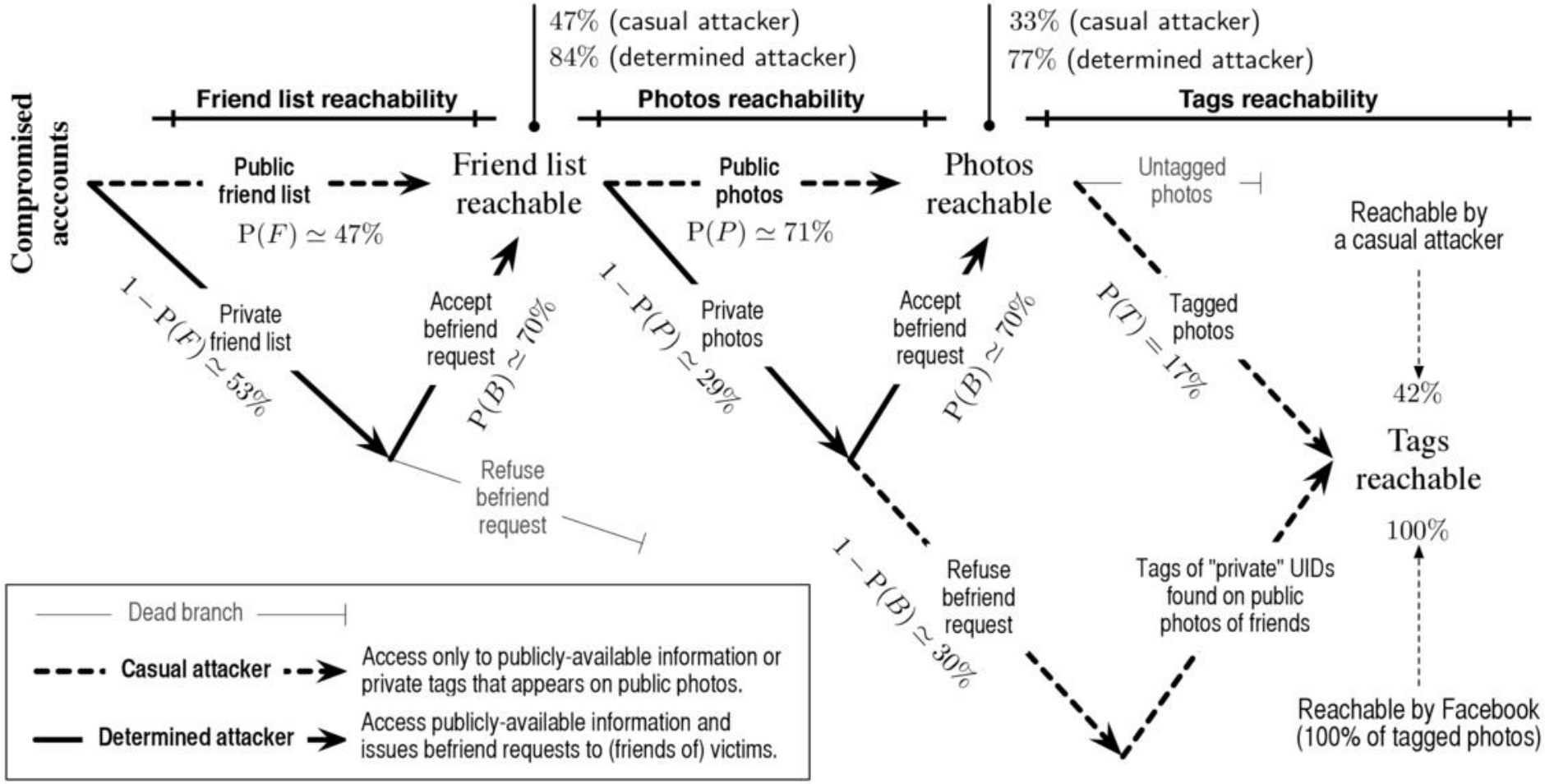
Attack tree to estimate the vulnerable FB population

Attack Surface Estimation – Photos



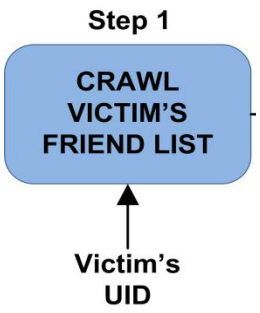
Attack tree to estimate the vulnerable FB population

Attack Surface Estimation – Tags



Attack tree to estimate the vulnerable FB population

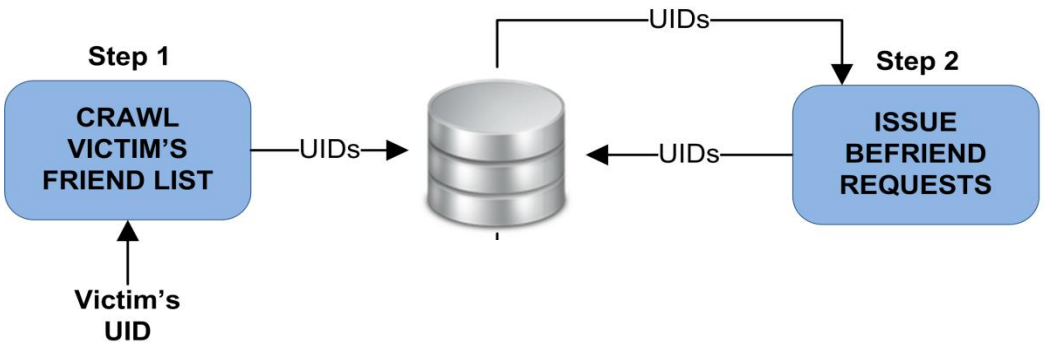
Automated Attack – 1



Preparatory Phase (offline)

1. Crawling Friend List

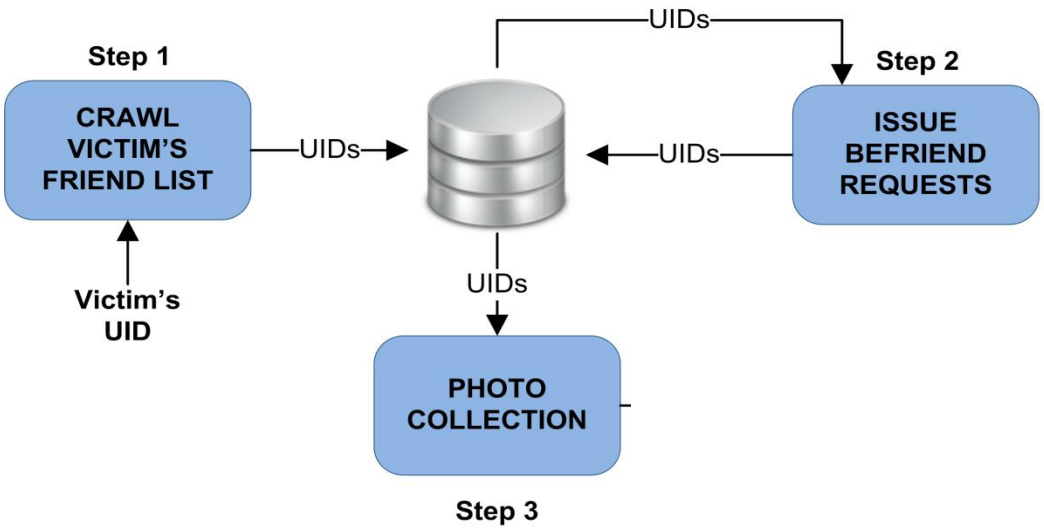
Automated Attack – 2



Preparatory Phase (offline)

1. **Crawling Friend List**
2. **Issuing Friend Requests** ***(optional)***
   - Creation of Fake Profiles
   - Infiltration in the Social Graph

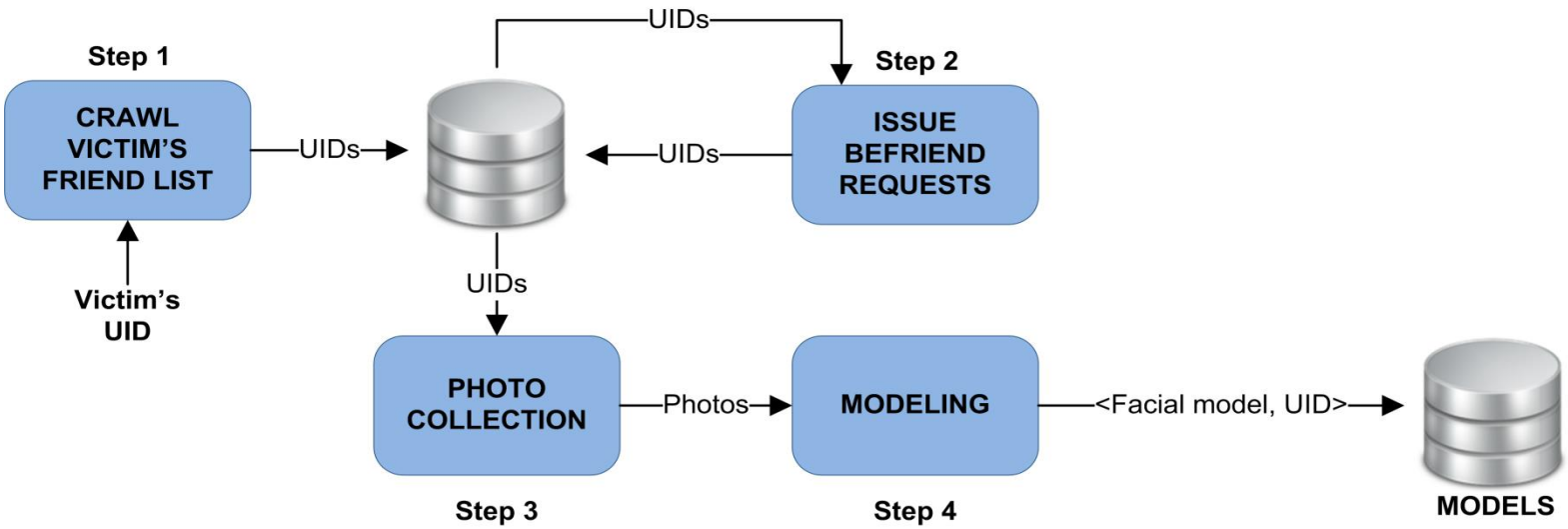
Automated Attack – 3



Preparatory Phase (offline)

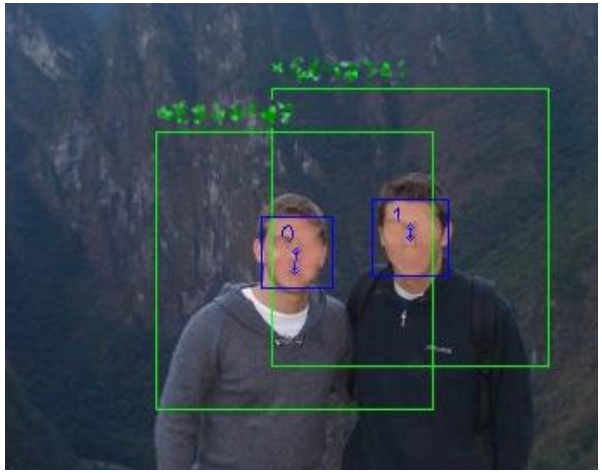
1. **Crawling Friend List**
2. **Issuing Friend Requests** ***(optional)***
   - Creation of Fake Profiles
   - Infiltration in the Social Graph
3. **Photo Collection** ***(public/private)***

Automated Attack – 4

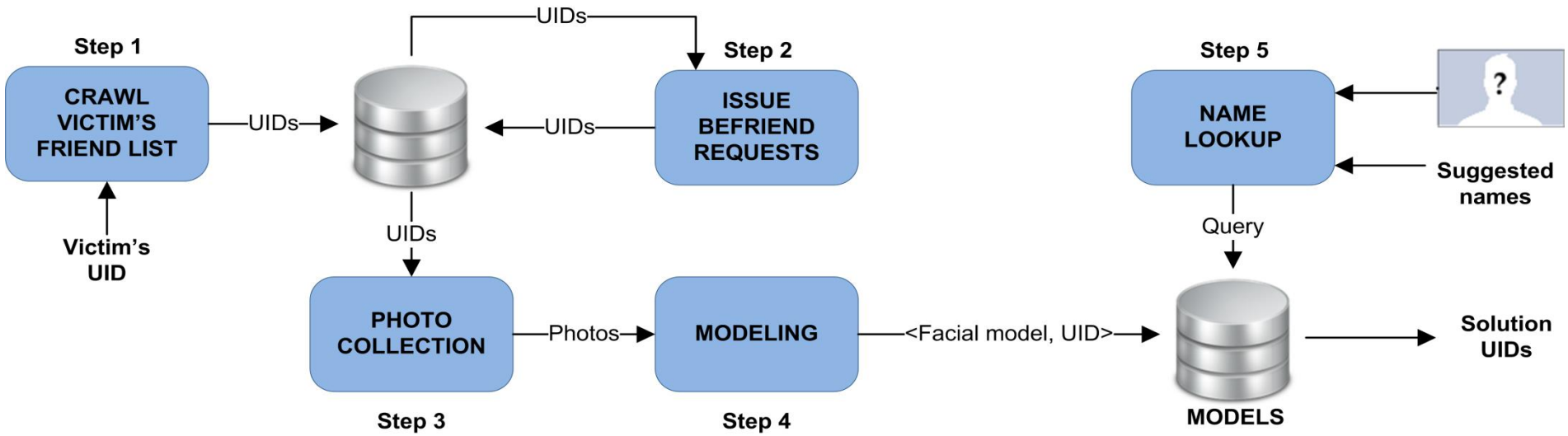


Preparatory Phase (offline)

1. **Crawling Friend List**
2. **Issuing Friend Requests** ***(optional)***
   - Creation of Fake Profiles
   - Infiltration in the Social Graph
3. **Photo Collection** ***(public/private)***
4. **Modeling**
   - Face Extraction and Tag Matching
   - Facial Modeling and Training



Automated Attack – 5



Preparatory Phase (offline)

1. **Crawling Friend List**
2. **Issuing Friend Requests** ***(optional)***
   - Creation of Fake Profiles
   - Infiltration in the Social Graph
3. **Photo Collection** ***(public/private)***
4. **Modeling**
   - Face Extraction and Tag Matching
   - Facial Modeling and Training

Execution Step (real-time)

5. **Name Lookup**

Experimental Evaluation

- We collect data as Casual Attackers (publicly available data)
- We have not compromised or damaged any user account

	TOTAL	PUBLIC	PRIVATE
UIDs	236,752	167,359	69,393
Not tagged	116,164	73,003	43,161
Tagged	120,588	94,356	26,232
Mean tags per UID:		19.39	10.58
Tags[9]	2,107,032	1,829,485	277,547
Photos	16,141,426	16,141,426	(not collected)
Albums	805,930	805,930	(not collected)

Summary of the collected dataset

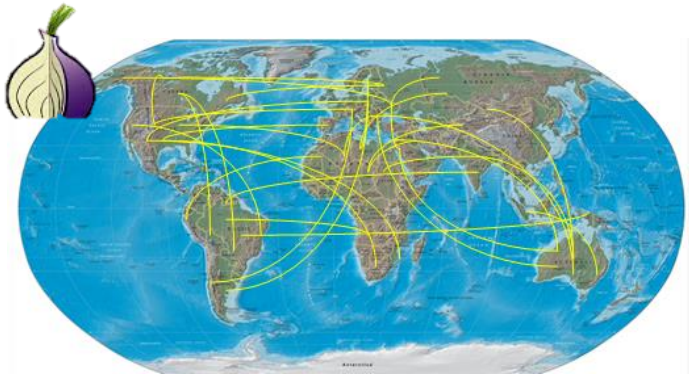
236,752 users

- 167,359 - **71% PUBLIC**
- 69,393 - 29% keep private albums
  - 38% (**11%** of total) **SEMI-PUBLIC**
  - 62% (**18%** of toal) **PRIVATE**

- CASUAL ATTACKER experiment
- DETERMINED ATTACKER experiment

Casual Attacker – Experiment

- **Used our fake accounts as "victims"**



- **Automated SA triggering through ToR**
  - Geographic dispersion of its exit nodes
  - Appear to be logging in from remote locations

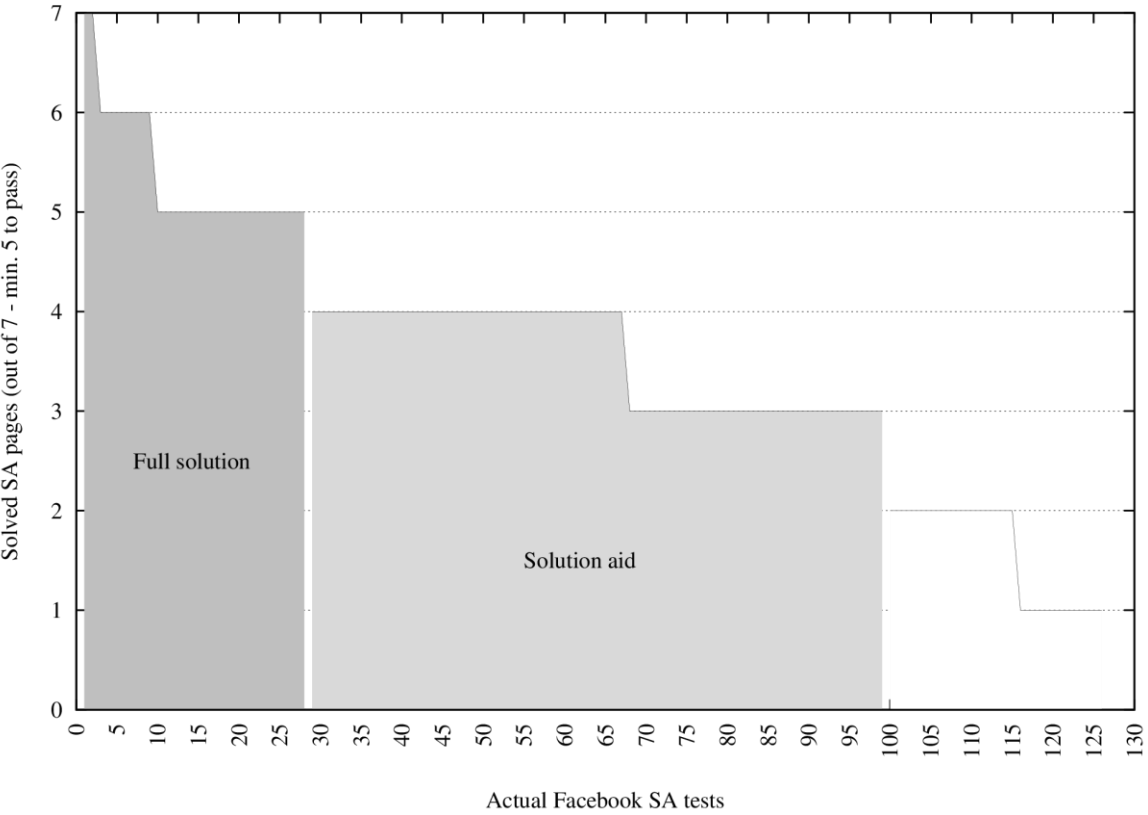
- **Face recognition: cloud service (face.com)**
  - Exposes REST API to developers
  - Superior accuracy

- ***Testing* dataset**
  - **127 real SA tests** collected

- ***Training* dataset**
  - From our dataset, we extracted information of the **1,131 distinct UIDs** that are friends with the fake profiles

	Training	Testing
Real SA tests	-	127
Photos	17,808	2,667
UIDs	1,131	5,335
Distinct UIDs	1,131	684

Casual Attacker – Accuracy



Solved SA pages out of the collected samples

~44 seconds to solve a complete test << 300 seconds

Manual verification

- **22% solved** (28/127)
- **56% need 1-2 guesses** (71/127)

78% in which

- Tests defeated or
- Obtained a significant advantage

Failed photos

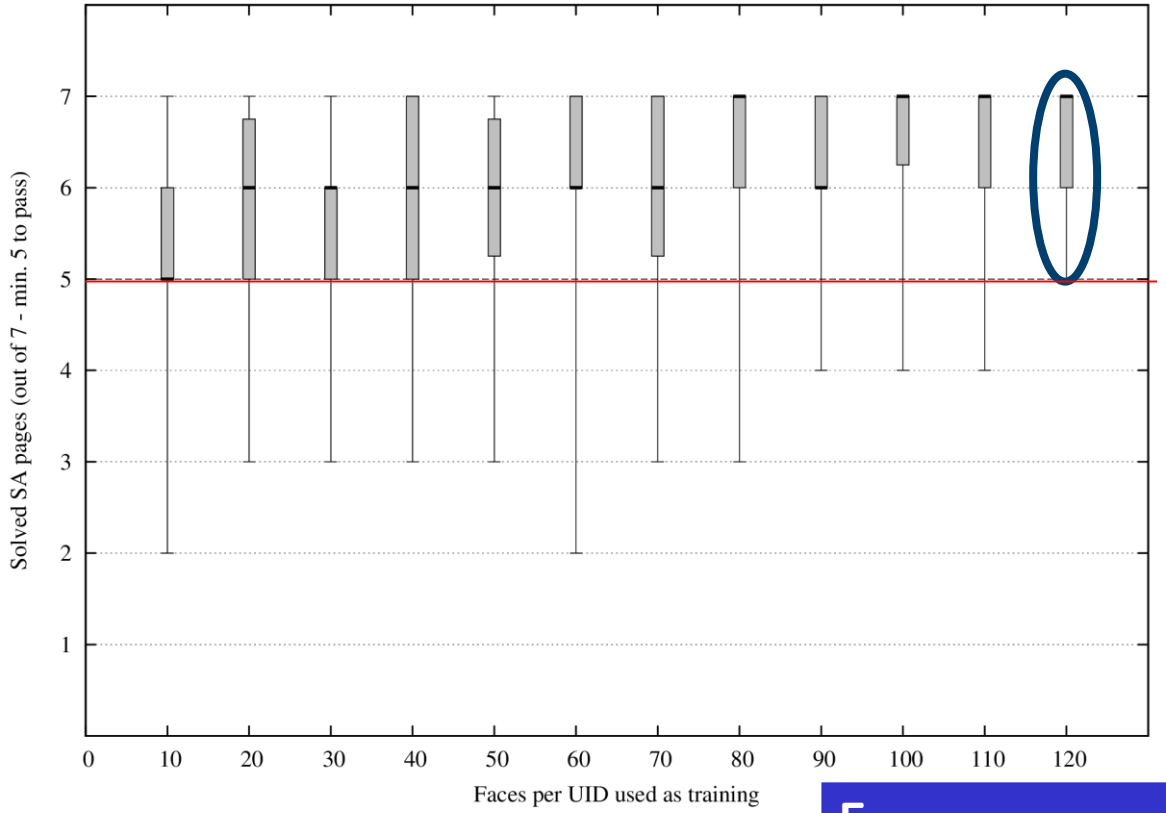
- 25% ***no face*** in photo
  - hard also for humans
- 50% ***unrecogn***. face
  - poor quality photos
- 25% ***no face model*** found

Determined Attacker – Experiment

- **Used simulation**
  - As only public data was used
  - Selected users with enough photos
- **Face recognition: custom implementation (OpenCV)**
  - Evaluate the accuracy and efficiency of our attack
  - Define number of faces per user needed to train a classifier to successfully solve the SA tests
  - Cons
    - Lower accuracy
    - Computational power required
- **Simulate SA tests from public photos**
  - Train system with **K = 10, 20, …, 120** faces per friend
  - **Generate 30 simulated SA tests** from photos not used for training

	TOTAL
UIDs	236,752
Tags	2,107,032
Photos	16,141,426
Albums	805,930

Determined Attacker – Accuracy



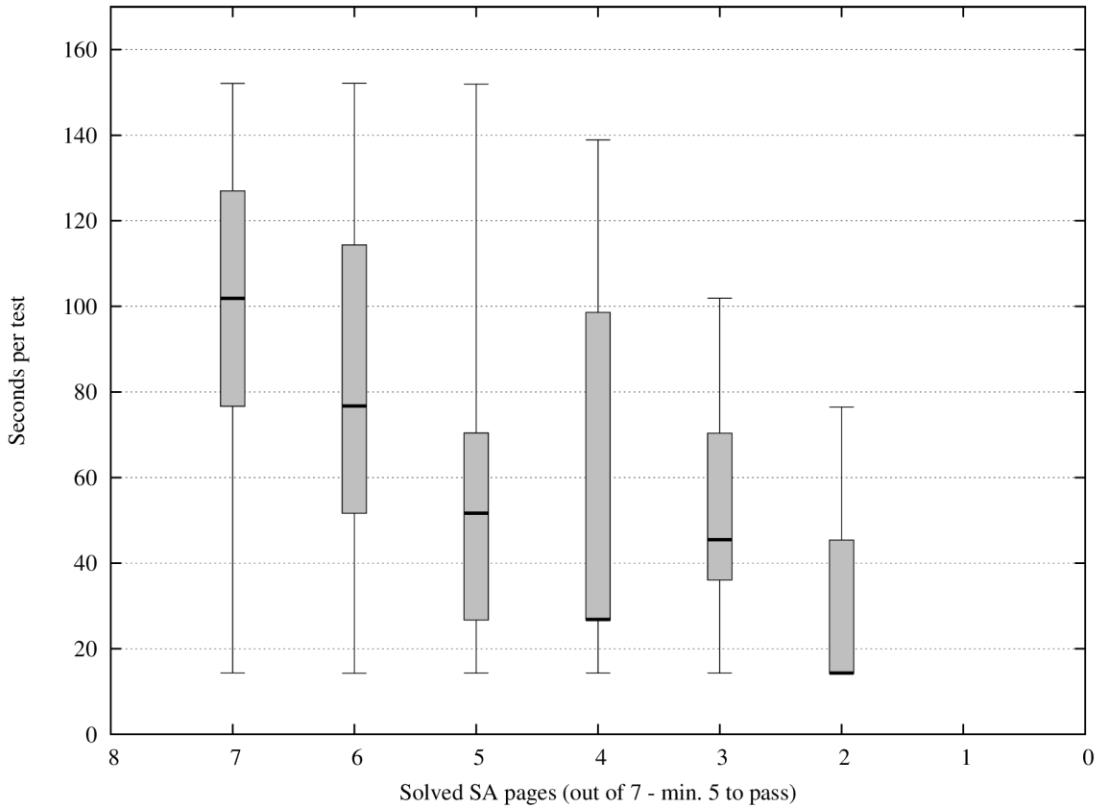
Solved SA pages as a function of the size of the training set

Always successful

- even when a scarce number of faces is available
- K > 100 ensures a more robust outcome

Faces	Min Success Rate
30	42%
90	57%
120	100%

Determined Attacker – Efficiency



Time required to lookup photos as a function of solved pages

Efficient

- time required for both "on the fly" training and testing remains within the 5-minute timeout

Max Time Required	Min Success Rate
100s	42%
140s	57%
150s < 300s	100%

Facebook's Response

- **We informed Facebook**
- **Acknowledged our results**
- **But**
  - Deployed SA to raise the bar in large-scale phishing attacks
  - Not designed for small-scale or targeted attacks

REDESIGN

reSA – "Social Authentication, Revisited"

[reSA]

- **Build SA tests from photos of poor quality**
  - State-of-the-art face recognition software detects human faces
  - But **cannot identify them** (people wearing glasses, etc.)

- **reSA**
  - 2FA scheme that can easily solved by humans but is robust against face-recognition software

- **By means of**
  - **Web application** that simulates the SA mechanism
  - **User study** where we asked humans to solve SA tests with photos of mixed quality

Photo Selection – Categories

Category	Faces	Description	Expectations Users	Expectations face.com	Model
Simple	Visibile	Faces with high confidence	Great results	Good results	SA
Medium	Not clearly visibile	Faces not identifiable by a software	Great/good results	Bad results	reSA
Difficult	Not visible	Photos with no human face detected	Mediocre results	Bad results	–

Easy *(Faces blurred for privacy reasons)

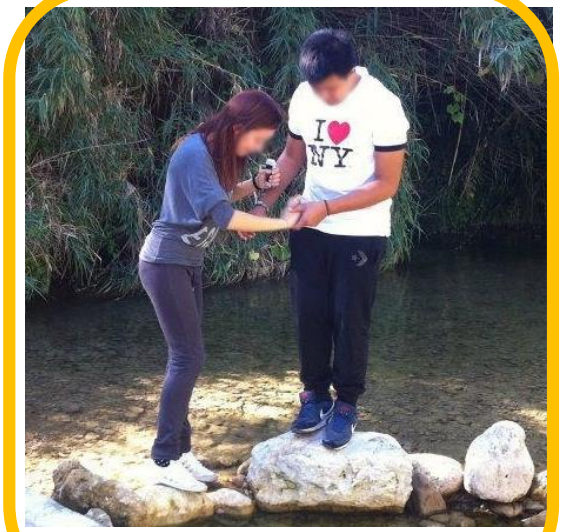
Medium

Difficult

Photo Selection – Categories

Category	Faces	Description	Expectations Users	Expectations face.com	Model
Simple	Visibile	Faces with high confidence	Great results	Good results	SA
Medium	Not clearly visibile	Faces not identifiable by a software	Great/good results	Bad results	reSA
Difficult	Not visible	Photos with no human face detected	Mediocre results	Bad results	–

Easy



Medium

Difficult

Photo Selection – Categories

Category	Faces	Description	Expectations Users	Expectations face.com	Model
Simple	Visibile	Faces with high confidence	Great results	Good results	SA
Medium	Not clearly visibile	Faces not identifiable by a software	Great/good results	Bad results	reSA
Difficult	Not visible	Photos with no human face detected	Mediocre results	Bad results	–

Easy

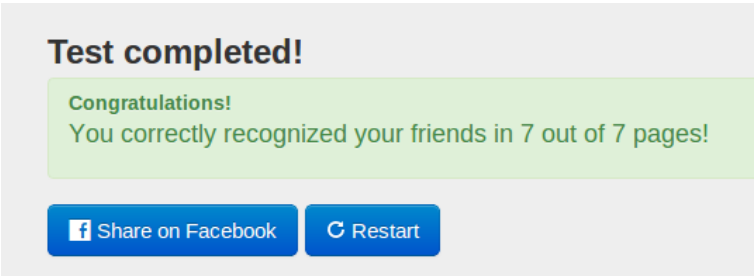
Medium

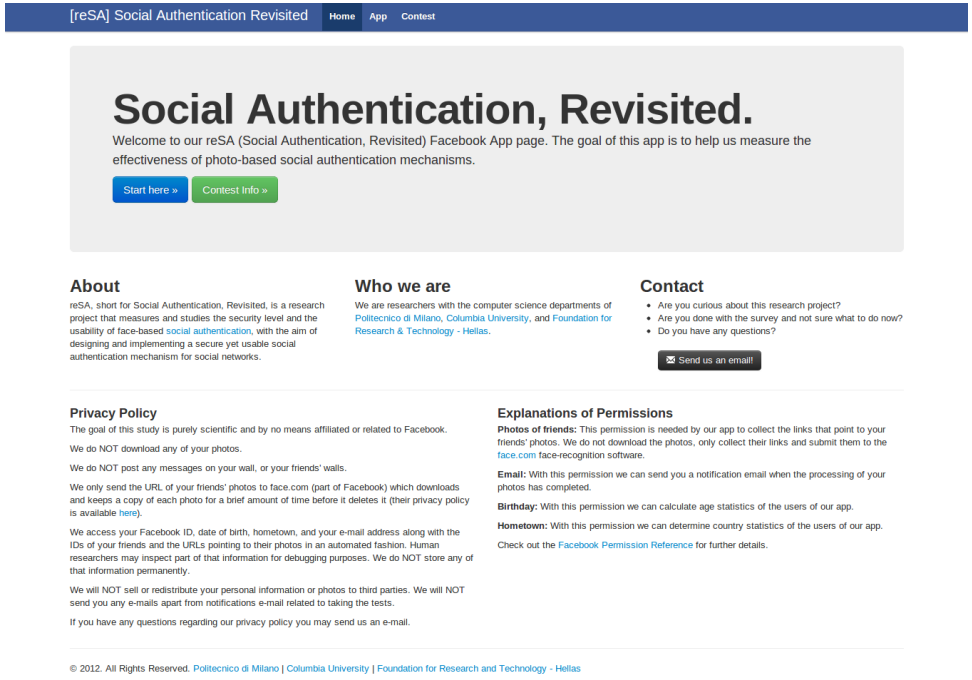
Difficult

User Study

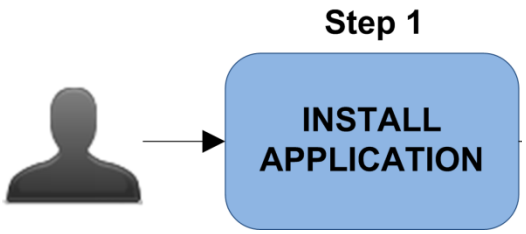
- **Measurement Application**
  - **Facebook app** that replicates the SA mechanism
  - Require users to identify their friends in SA challenges, and complete a questionnaire for each photo

- **Recruiting users**
  - ✗ **Amazon Mechanical Turk** (AMT)
  - ✓ User incentives
    - **Gamification**
    - **Prizes**





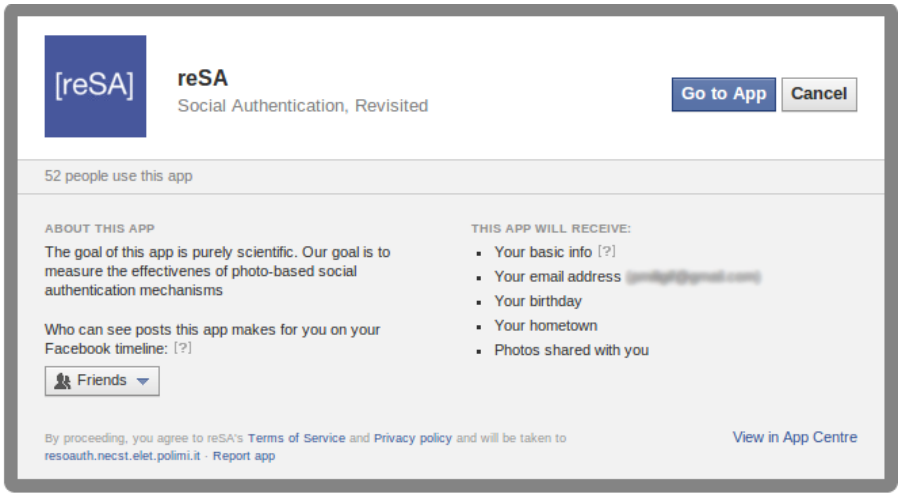
System Overview – 1



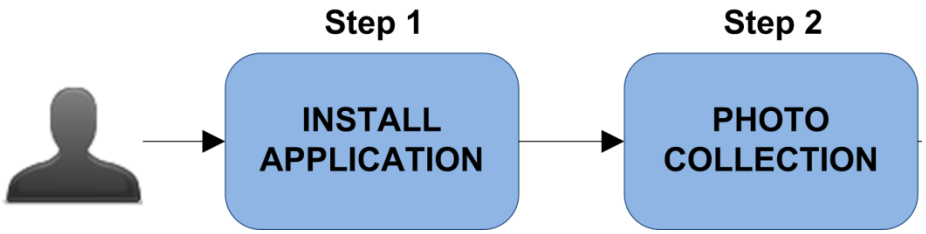
Preparation Phase

(collect and prepare all the information needed for the actual creation of the tests)

1. Application Installation/**Authorization**



System Overview – 2



Preparation Phase

1. Application Installation/**Authorization**
2. **Photo** Collection
   I. Obtain list of his friends
   II. Collect all the tags of user's friends
   III. Download corresponding photos

Listing 4.1: FQL query that retrieves a user's friendlist

```
SELECT uid, name, sex FROM user WHERE uid=me() OR
    uid IN (SELECT uid2 FROM friend WHERE uid1=me())
```

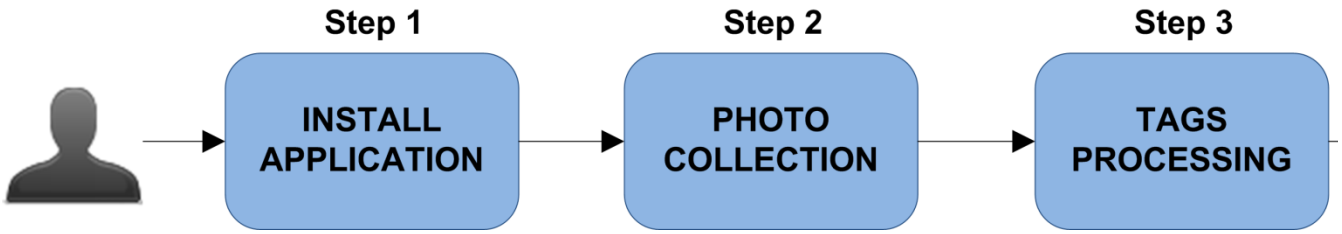
Listing 4.2: FQL query that retrieves all the tags of a user

```
SELECT pid, subject, text, xcoord, ycoord
    FROM photo_tag WHERE subject=FRIEND_UID
```

Listing 4.3: FQL query that retrieves the metadata of a given photo

```
SELECT pid, aid, link, images FROM photo WHERE pid=PHOTO_PID
```

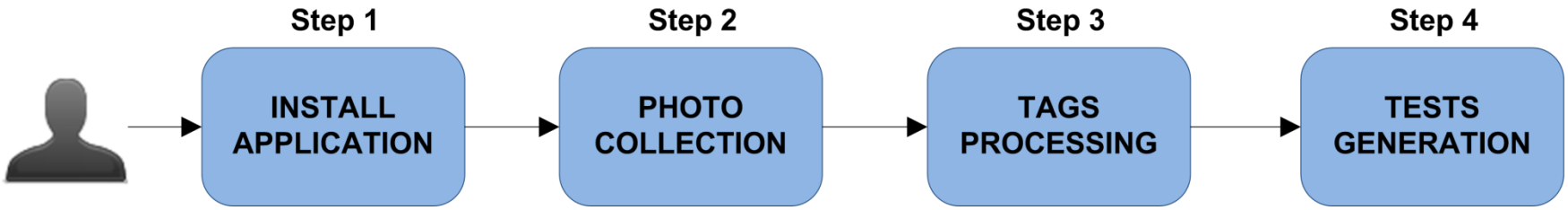
System Overview – 3



Preparation Phase

1. Application Installation/**Authorization**
2. **Photo** Collection
3. **Tags** Processing
   I. **Category** Assignment
      - Process each photo to identify faces
      - Categorize them based on the quality of the faces found
   II. **Eligibility** Checks
      - At least 7 friends eligibile for each type
      - A friend is "*eligible*" if he has at least 3 tags that satisfy the requirements of a kind of test

System Overview – 4



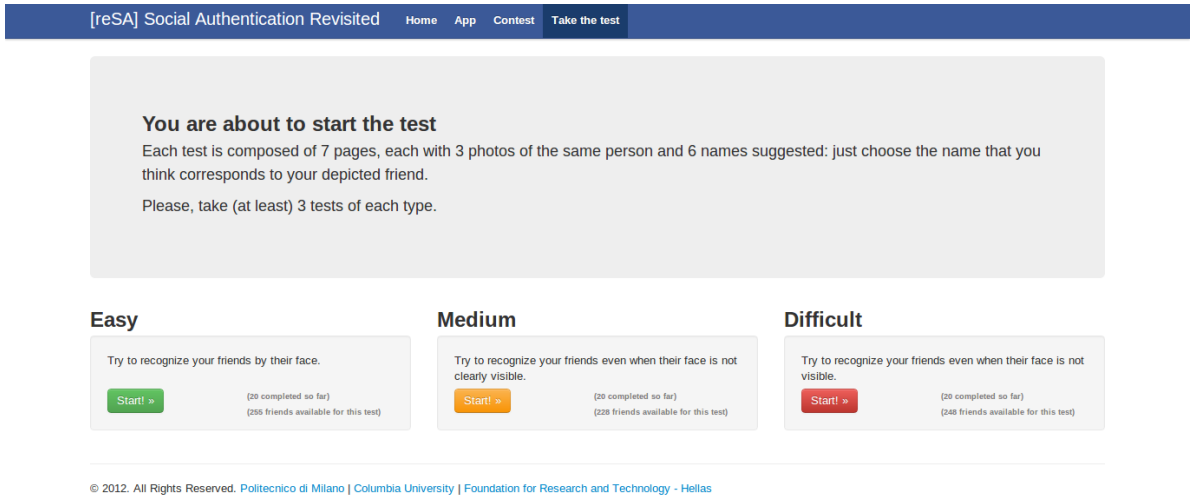
Preparation Phase

1. Application Installation/**Authorization**
2. **Photo** Collection
3. **Tags** Processing

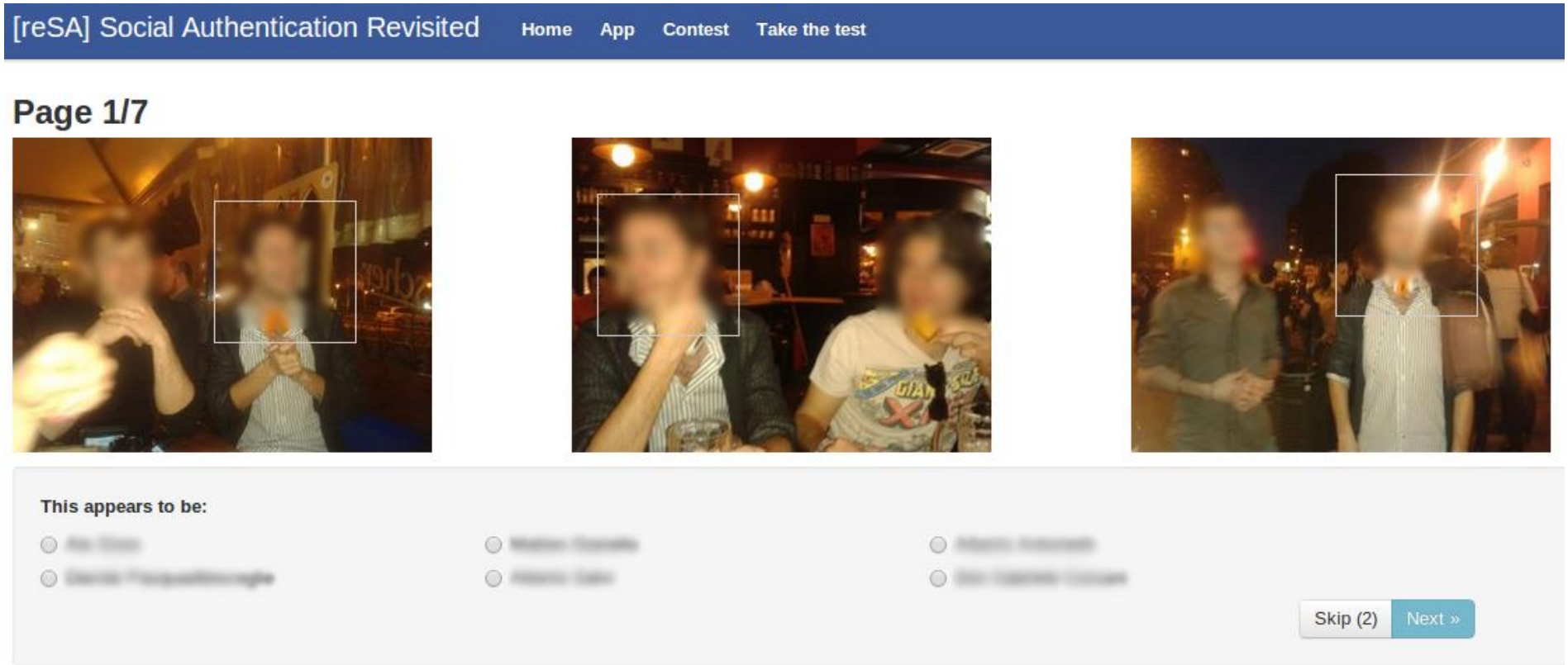
Tests Generation

(on-request)

- Choose category



Example – Challenge



Example – Survey

[reSA] Social Authentication Revisited Home App Contest Take the test

Page 1/7 - Tag Analysis

Congratulations!
You correctly identified [illegible]!

We will show you the photos again and ask you some questions about each one

Type of photo

- Portrait
- Landscape
- Objects
- Text
- Animals
- Art

Where's [illegible] Face?

- [illegible] face is **within** the square and is **clearly visible**
- [illegible] face is **outside** the square and is **clearly visible**
- [illegible] face is **within** the square, but **not clearly visible**
- [illegible] face is **outside** the box, but **not clearly visible**
- [illegible] face is **not in the photo** at all

Faces in the photo

- There are **other people's faces both outside and inside** the square (not [illegible])
- There's **someone else's face within** the square (not [illegible])
- There's **someone else's face outside** of the square (not [illegible])
- There are **no other faces** in this photo
- There are **no faces** in this photo

Why was this photo useful for identifying [illegible]?

- I remember seeing this photo from [illegible]
- The content of the photo is relevant to [illegible]
- None of the other suggested friends matched
- This photo was not useful
- [illegible] is in the photo

Dataset

- **Demographics**
  - **141 users** (120 males and 21 females)
  - **14 different countries** (majority from Italy and Greece)
  - Age comprised from **20 and 40 years**

- **Collected data**
  - **4,5M photos** and **5M tags**
    - 2.066.386 tags can be used for the simple category
    - 593.479 for the medium
    - 820.947 for thr difficult
    - 1.6M tags doesn't satisfy any selection criteria

Country	Number
Italy	96
Greece	16
Spain	6
United Kingdom	6
Germany	3
United States	3
Colombia	2
France	2
India	2
Czech Republic	1
Dominican Republic	1
Syria	1
Turkey	1
Ukraine	1

Distribution of users by country

Type	Total	Mean
Photo	4,457,829	31,615
Tags	5,087,034	36,078
Simple	2,066,386	14,655
Medium	593,479	4,209
Difficult	820,947	5,822
Useless	1,606,222	11,391

Summary of the collected dataset

Results – Tests taken

Type	Total	Passed	Success	Per User
Simple	362	358	98.89%	3.98
Medium	347	344	99.14%	3.81
Difficult	335	275	82.09%	3.68
Total	1044	977	93.58%	11.47

Summary of the collected SA tests

- Our users took a total number of **1,044 distinct SA tests** (avg of 11 tests taken by each)

Results – Simple & Medium

Type	Total	Passed	Success	Per User
Simple	362	358	98.89%	3.98
Medium	347	344	99.14%	3.81
Difficult	335	275	82.09%	3.68
Total	1044	977	93.58%	11.47

Summary of the collected SA tests

- Our users took a total number of **1,044 distinct SA tests** (avg of 11 tests taken by each)
- **Simple** and **medium** categories
  - obtained great results from users
  - success rate that span across 98% and 99%

Results – Difficult

Type	Total	Passed	Success	Per User
Simple	362	358	98.89%	3.98
Medium	347	344	99.14%	3.81
Difficult	335	275	82.09%	3.68
Total	1044	977	93.58%	11.47

Summary of the collected SA tests

- Our users took a total number of **1,044 distinct SA tests** (avg of 11 tests taken by each)
- **Simple** and **medium** categories
  - obtained great results from users
  - success rate that span across 98% and 99%
- **Difficult** category
  - users encountered more problems
  - but also score surprisingly well (success rate that decreases until 82%)

Results – Outcome

Type	Total	Passed	Success	Per User
Simple	362	358	98.89%	3.98
Medium	347	344	99.14%	3.81
Difficult	335	275	82.09%	3.68
Total	1044	977	93.58%	11.47

Summary of the collected SA tests

People are able to recognize their friends
just as good in both standard SA tests and tests with photos of poor quality

We propose the use of tests with photos of poor quality as that will
increase security without affecting usability

CONCLUSIONS

Conclusions

- **Demonstrated the weaknesses of SA**
- **Designed and implemented an automated SA breaking system**
  - **Publicly-available data** sufficient for attackers
  - **Cloud services** can be utilized effectively
  - **Facebook** should reconsider its threat model

- **Need to revisit the SA approach**
- **Designed and implemented a secure yet usable SA mechanism**
  - 2FA scheme that can easily solved by humans but is **robust against face-recognition software**
  - People are able to recognize their friends **just as good in both standard SA tests and tests with photos of poor quality**

Acknowledgments

Joint work within the **SysSec EU Network of Excellence**

- **Politecnico di Milano**
- Columbia University
- FORTH Research Center

syssec

POLITECNICO DI MILANO

FORTH
Foundation for Research & Technology, Hellas

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

THANK YOU.