ALL YOUR FACE ARE BELONG TO US

BREAKING FACEBOOK'S SOCIAL AUTHENTICATION

FEDERICO MAGGI

NECSTLAB, POLITECNICO DI MILANO

ABOUT THE TITLE

"All Your Face are Belong to Us"

JAPANESE-TO-ENGLISH TRANSLATION ERROR

EU EDITION OF "ZERO WING" CONSOLE GAME, 1991

BECAME AN INTERNET MEME, 2000

CATS：連邦政府軍のご協力により、君達の基地は、全てCATSがいただいた。

CATS: All your base are belong to us.

CATS: With the cooperation of Federation Forces,
all of your bases now belong to us.

CATS: ALL YOUR BASE ARE BELONG
TO US.

MARCO LANCINI
FEDERICO MAGGI
STEFANO ZANERO
POLITECNICO DI MILANO, ITALY

JOINT WORK

ACCEPTED AT ACSAC 2012

COLUMBIA UNIVERSITY, US
GEORGIOS KONTAXIS
ANGELOS KEROMYTIS

FORTH, GREECE
JASON POLAKIS
SOTIRIS IOANNIDIS

ONLINE SOCIAL NETWORKS

ONLINE SOCIAL NETWORKS (2013)

	Registered Users	Active Users
Facebook	1+ billion	1 billion
Tencent QQ	784+ million	712 million
Google+	500+ million	235 million
Twitter	500+ million	200+ million
Linkedin	200+ million	160 million
Tencent Qzone	597+ million	150 million
Sina Weibo	400+ million	100+ million
Windows Live	100 million	100 million
Instagram	100+ million	100 million

Wikipedia

"List of virtual communities with more than 100 million active users"

ONLINE SOCIAL NETWORKS

FACEBOOK REACHED 1+ BILLION ACTIVE USERS

1/7th OF THE WORLD POPULATION

MASSIVE USER BASE

APPEALING TARGET FOR ONLINE CRIME

ONLINE SOCIAL NETWORKS ABUSED

IDENTITY THEFT

SPAMMING

PHISHING

~~SELLING CREDIT CARDS~~ SELLING STOLEN ACCOUNTS

MALICIOUS FACEBOOK ACCOUNTS

97% ARE REAL, COMPROMISED ACCOUNTS

Gao et al.
"Detecting and Characterizing Social Spam Campaigns"
ACM Internet Measurement Conference, 2010

MAIN CAUSES OF STOLEN ACCOUNTS

INFORMATION-STEALING MALWARE

SOCIAL ENGINEERING

PHISHING

KEEPING STOLEN ACCOUNTS SAFE

MULTI-FACTOR AUTHENTICATION

SOMETHING YOU KNOW: A PASSWORD

SOMETHING YOU HAVE: A TOKEN

Paul Applegate

http://www.flickr.com/photos/mrapplegate/1287965486/

DRAWBACKS

LOW ACCEPTANCE

CUMBERSOME

CAN BE LOST

FACEBOOK'S APPROACH

~~SOMETHING YOU HAVE (TOKEN)~~

SOMEONE YOU KNOW (FRIEND)

facebook Sign Up

Facebook Login

Email or Phone: me@example.com

Password: ••••••••••

Keep me logged in

Log In or Sign up for Facebook

Forgot your password?

Italiano English (US) Español Português (Brasil) Français (France) Deutsch العربية हिन्दी 中文(简体)

Mobile Find Friends Badges People Pages Places Apps Games Music
About Create an Ad Create a Page Developers Careers Privacy Cookies Terms Help

"A CONTINUED COMMITMENT TO SECURITY"

https://www.facebook.com/blog/blog.php?post=486790652130

This appears to be:

- Naitik Shah
- Tim Kuper
- Alok Menghrajani
- Nick Wilkerson
- David Starling
- Alessio Riso

Submit | Skip ▸ (2 skips left)

WHEN DOES IT COME INTO PLAY?

GEO LOCATION THAT YOU NEVER ACCESSED FROM

FIRST TIME YOU USE A COMPUTER

HOW DOES IT WORK?

7 FRIENDS TO IDENTIFY

3 PHOTOS PER FRIEND

6 SUGGESTIONS

2 MISTAKES

GROUND TRUTH FRIENDS → PHOTOS → TAGS

ADVANTAGES OF SOCIAL AUTHENTICATION

PEOPLE ACCUSTOMED TO TAGGING FRIENDS

MORE USER FRIENDLY THAN A TOKEN

LOOKS LIKE A GAME

ADVERSARY MODEL

ANYONE OUTSIDE THE VICTIM'S SOCIAL CIRCLE

A STRANGER

~~CLOSE COMMUNITIES~~

~~CLOSE FRIENDS~~

~~FAMILY~~

ASSUMPTION

THE ATTACKER CANNOT INFILTRATE
INTO THE VICTIM'S SOCIAL CIRCLE

SECURITY WEAKNESSES

5 FRIENDS TO IDENTIFY

3 PHOTOS PER FRIEND

6 SUGGESTIONS

2 MISTAKES

This information is publicly available to some degree.

CAN AN ATTACKER BYPASS SOCIAL AUTHENTICATION AUTOMATICALLY?

(#1 CASUAL ATTACKER)

FRIENDS

SECURITY WEAKNESSES TAKE 2

~~7~~ 5 FRIENDS TO IDENTIFY

3 PHOTOS PER FRIEND

6 SUGGESTIONS

~~2 MISTAKES~~

GROUND TRUTH FRIENDS → PHOTOS → TAGS

PUBLIC FRIENDS LIST

"Are friend lists publicly reachable?"

47% OF USERS LEAVE THEIR FRIEND LIST PUBLIC

R. Dey at al.
Facebook users have become much more private: A large-scale study.
IEEE Workshop on Security and Social Networking, 2012

CAN AN ATTACKER BYPASS SOCIAL AUTHENTICATION AUTOMATICALLY?

(#2 DETERMINED ATTACKER)

ACCEPT BEFRIEND REQUESTS?

100%-47% = 53% OF USERS LEAVE THEIR FRIEND LIST PRIVATE

70% OF USERS ACCEPT BEFRIEND REQUESTS BLINDLY

D. Irani et al.
Reverse social engineering attacks in online social networks.
DIMVA 2011

MATH: FRIEND LIST REACHABILITY

47% OF USERS LEAVE THEIR FRIEND LIST PUBLIC

53% OF USERS LEAVE THEIR FRIEND LIST PRIVATE

70% OF USERS ACCEPT BEFRIEND REQUESTS BLINDLY

47% + 53% * 70%

84% OF THE USERS

GROUND TRUTH FRIENDS → PHOTOS → TAGS

84%

PHOTOS

PUBLIC PHOTOS: A CLOSER LOOK

"Are photos publicly reachable?"

71% OF THE USER LEAVE THEIR PHOTOS PUBLIC

GROUND TRUTH FRIENDS ⟶ PHOTOS ⟶ TAGS

We measured this on a sample of 236,752 Facebook users.

MATH: PHOTO REACHABILITY

71% OF THE USER LEAVE THEIR PHOTOS PUBLIC

29% OF USERS LEAVE THEIR PHOTOS PRIVATE

70% OF USERS ACCEPT BEFRIEND REQUESTS BLINDLY

84% * (71% + 29% * 70%)

77% OF THE USERS

GROUND TRUTH FRIENDS → PHOTOS → TAGS

84% 77%

TAGS

PUBLIC TAGS

"Are tags publicly reachable?"

42% OF THE TAGS ARE REACHABLE

PUBLIC TAGS + PRIVATE TAGS ON PUBLIC PHOTOS

GROUND TRUTH FRIENDS → PHOTOS → TAGS

We measured this on a sample of 236,752 Facebook users.

GROUND TRUTH FRIENDS → PHOTOS → TAGS

84% 77% 42%

THE GUESS SPACE FOR
AN ATTACKER IS NARROW.

COULD AN ATTACKER NARROW IT FURTHER?

PHOTOS TAKE 2

PUBLIC PHOTOS A CLOSER LOOK

"Does Facebook select the photos for social auths?"

82% OF PHOTOS IN SOCIAL AUTH. CONTAIN FACES

VS.

ONLY 69% OF PHOTOS CONTAIN FACES OVERALL

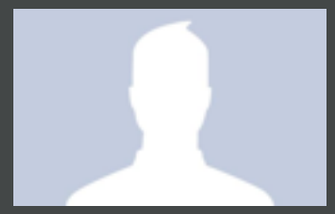
GROUND TRUTH FRIENDS → PHOTOS → TAGS

We measured this on a sample of 6,115 photos.

FACEBOOK PICKS

PHOTOS THAT CONTAIN FACES.

82%



GROUND TRUTH → FRIENDS → PHOTOS → TAGS

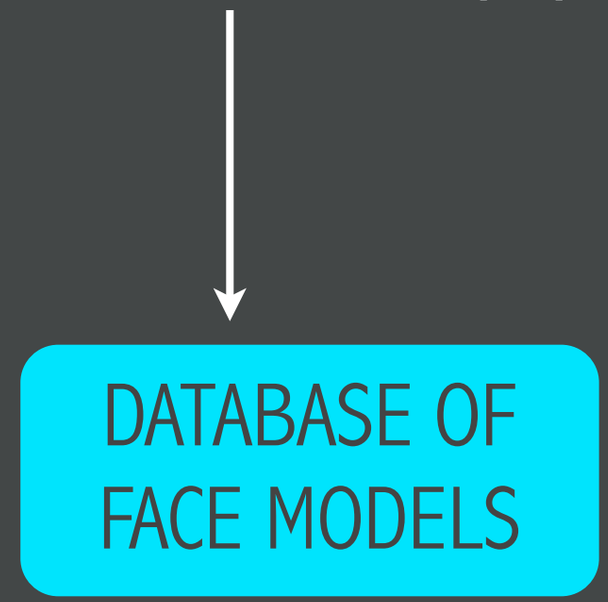
84% 77% 42%

PRACTICAL ATTACK STEP1

CRAWLING FRIENDS LIST OF THE VICTIM (1)

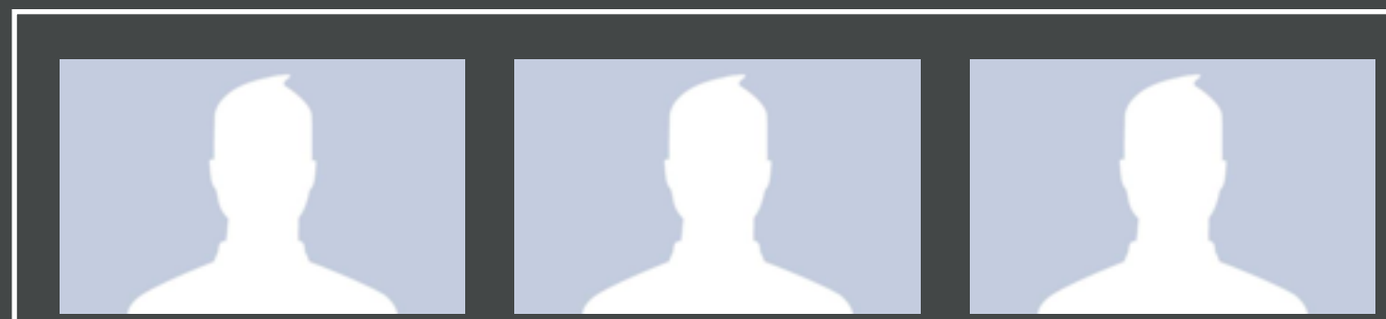
COLLECTING THEIR TAGGED PHOTOS (2)

FACE MODELING (3)



PRACTICAL ATTACK STEP2

SOCIAL AUTHENTICATION



NAME! ← FACE RECOGNITION ← PHOTO

DATABASE OF FACE MODELS

FACE MODELING AND RECOGNITION

what did we use?


face.com

face.com acquired by facebook

AH...THE IRONY

SO, AN ATTACKER COULD EVEN USE FACEBOOK'S OWN TECHNOLOGY TO BYPASS ITS SOCIAL AUTHENTICATION

EXPERIMENTAL EVALUATION

CASUAL ATTACKER

ONLY PUBLICLY AVAILABLE INFORMATION

NO BEFRIEND REQUESTS

SUCCESS OF THE CASUAL ATTACKER

22% FULL SOLUTION

56% 1–2 GUESSES NEEDED

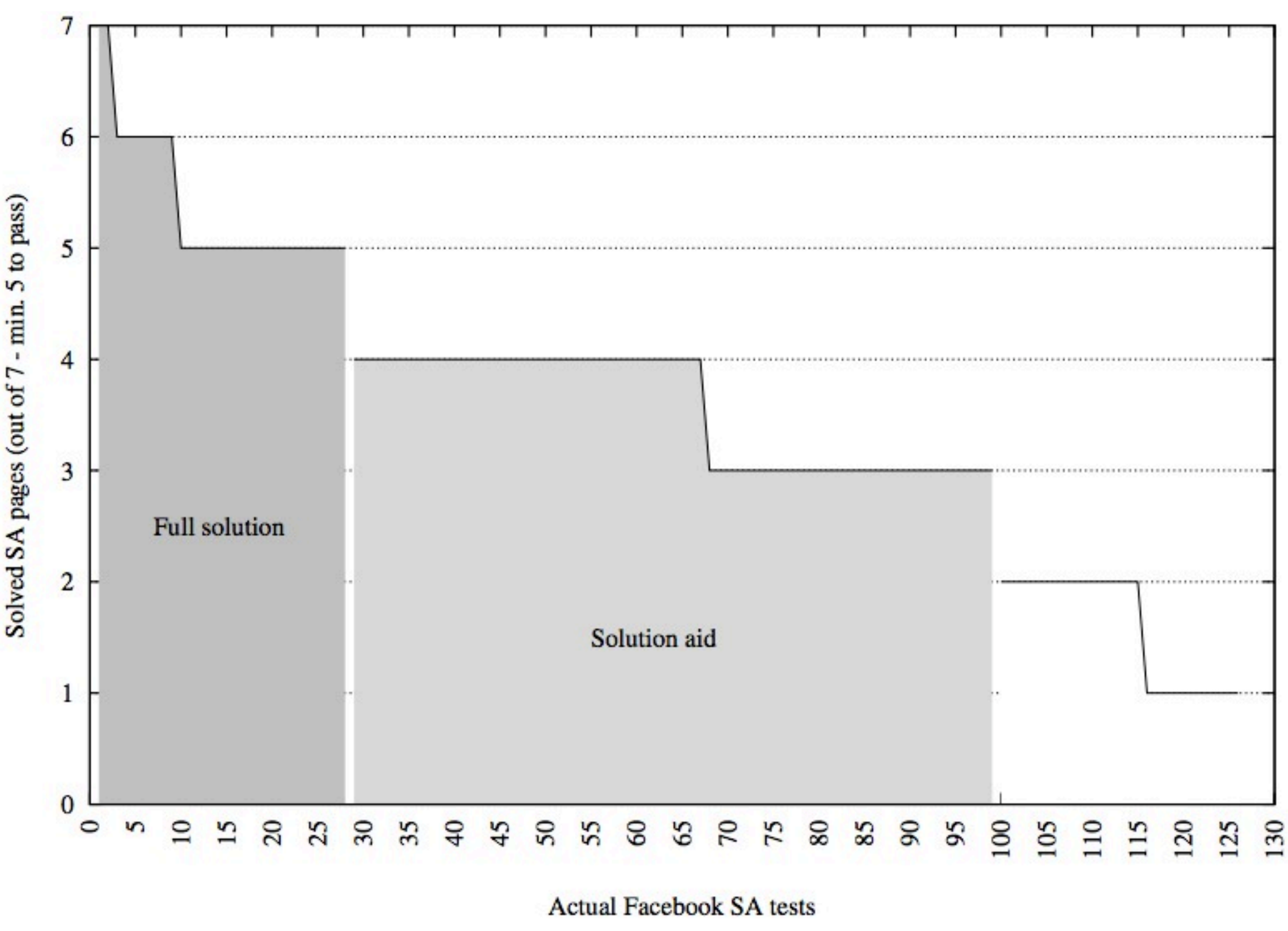
78% OVERALL (2 MISTAKES ALLOWED)

WHEN THE CASUAL ATTACKER FAILS

25% NO FACES IN THE PHOTOS

50% UNRECOGNIZABLE FACE

25% NO FACE MODEL FOUND


Solved SA pages (out of 7 - min. 5 to pass)
7
6
5
4
3
2
1
0
Full solution
Solution aid
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
Actual Facebook SA tests

EXPERIMENTAL EVALUATION

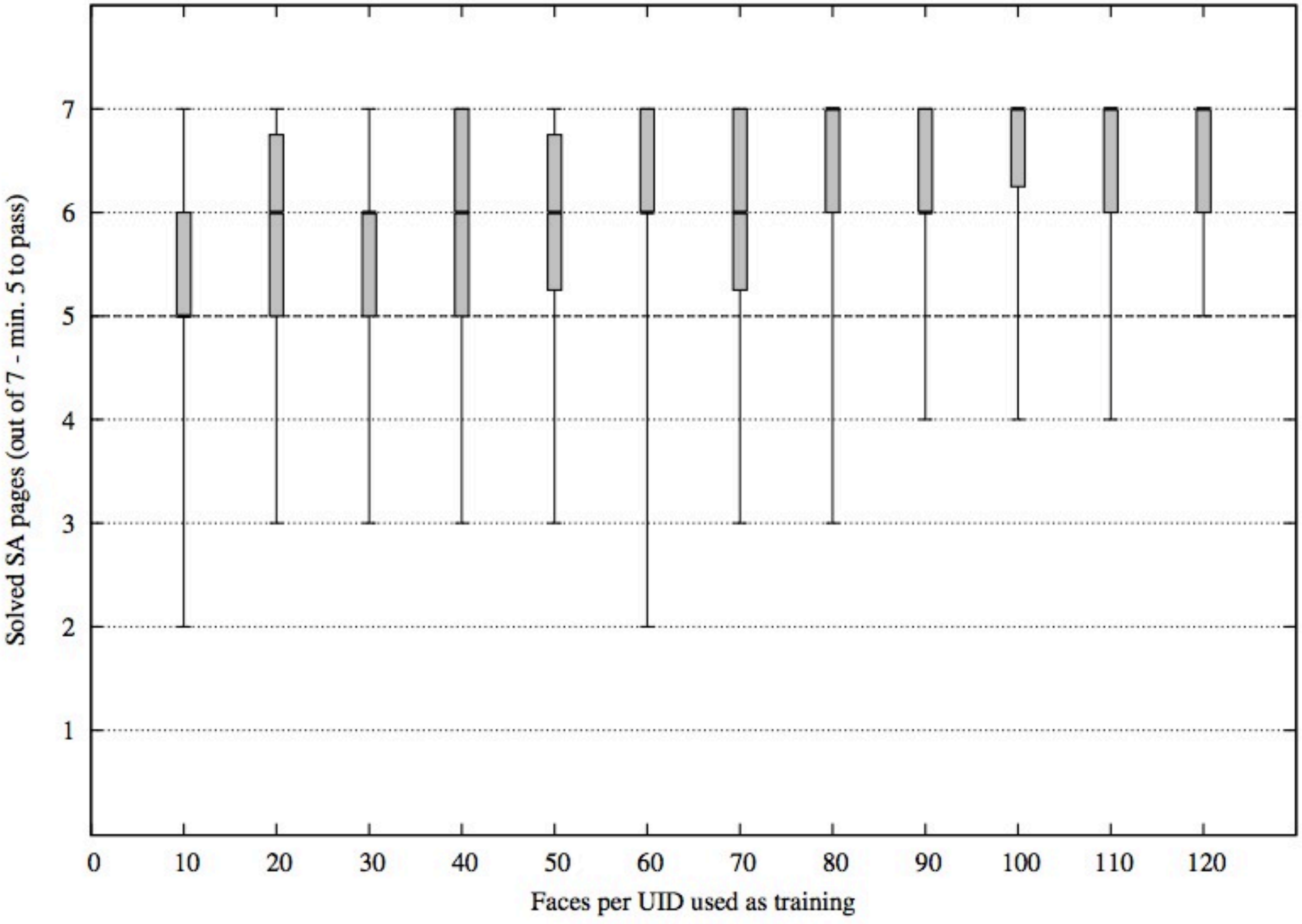
DETERMINED ATTACKER

ACCESS TO 77% OF THE PHOTOS

EMULATED OFFLINE

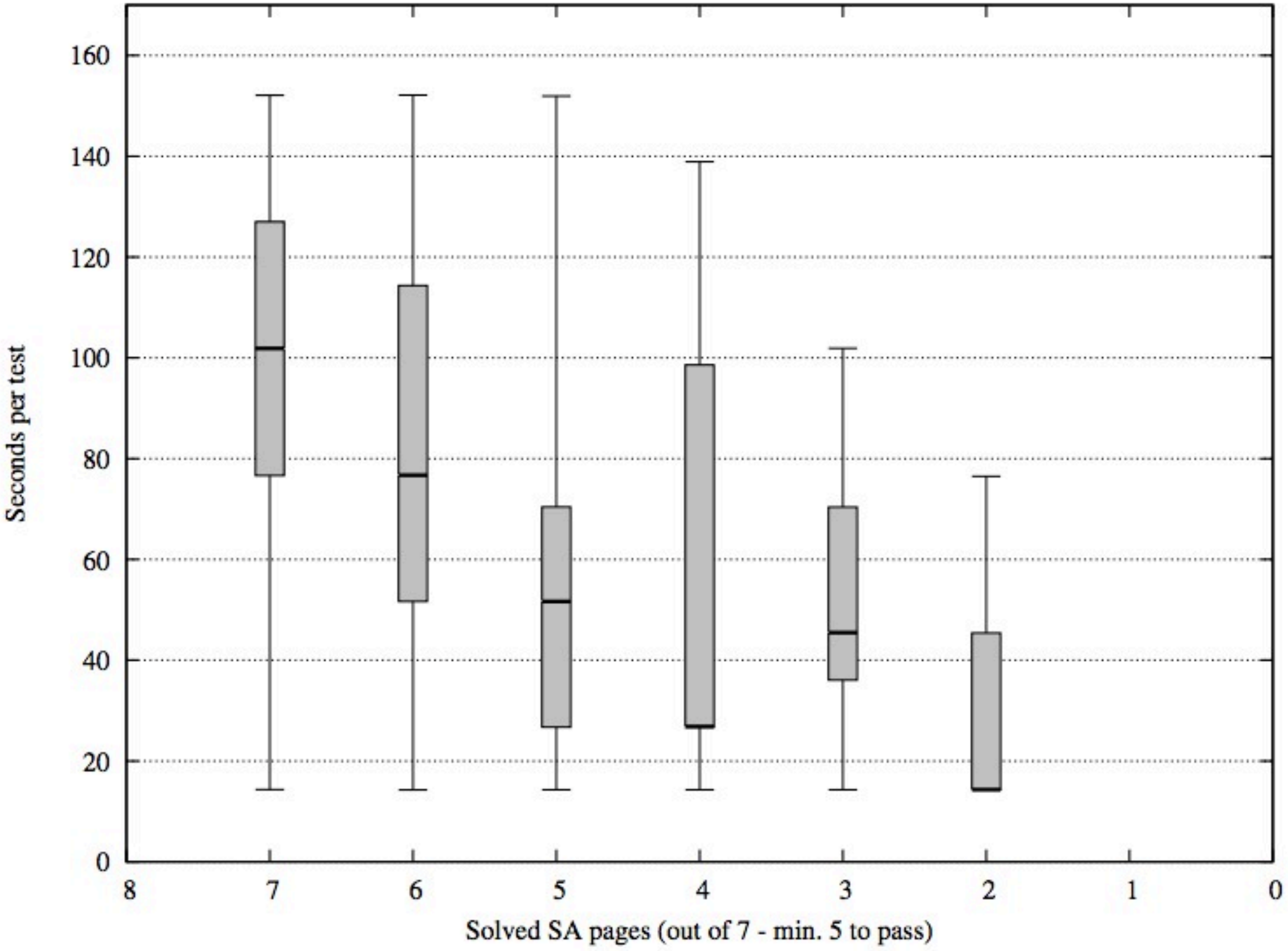
SUCCESS OF THE DETERMINED ATTACKER

FACES CRAWLED	MINIMUM SUCCESS RATE
30	42%
90	57%
120	100%


Solved SA pages (out of 7 - min. 5 to pass)
7
6
5
4
3
2
1
0
10
20
30
40
50
60
70
80
90
100
110
120
Faces per UID used as training

SPEED OF THE DETERMINED ATTACKER

MAX TIME REQUIRED	MINIMUM SUCCESS RATE
100s	42%
140s	57%
150s < TIMEOUT	100%


160
140
120
100
80
60
40
20
0
Seconds per test
8
7
6
5
4
3
2
1
0
Solved SA pages (out of 7 - min. 5 to pass)

FACEBOOK RESPONSE

ACKNOWLEDGED OUR RESULTS

SOCIAL AUTH. MEANT AS A "WEAK" PROTECTION

INEFFECTIVE AGAINST TARGETED ATTACKS

USERS CAN USE LOGIN APPROVAL (WHO DOES IT?)

QUICK REMEDIATIONS

OPT-IN LOGIN APPROVAL (USERS)

REMOVE SUGGESTIONS (FACEBOOK)

REDUCE TIMEOUT (FACEBOOK)

RETHINKING SOCIAL AUTHENTICATION

PEOPLE CAN RECOGNIZE THEIR FRIENDS "LOOK"

USE PHOTOS WITH NO FACES

~~FACE RECOGNITION~~

CONCLUSIONS

SOCIAL AUTH. INEFFECTIVE FOR 84% OF THE USERS

THREAT MODEL EXCLUDES OUR TARGETED ATTACK

CLOUD-BASED FACE-RECOGNITION MADE IT EASIER

SOCIAL AUTHENTICATION SHOULD BE REVISITED

THANK YOU!

CATS: ALL YOUR ~~BASE~~ FACE ARE BELONG TO US.

FEDERICO MAGGI: @PHRETOR
HTTP://MAGGI.CC