rtCaptcha: A Real-Time Captcha Based Liveness Detection System

Erkam Uzun, Simon Pak Ho Chung, Irfan Essa, Wenke Lee

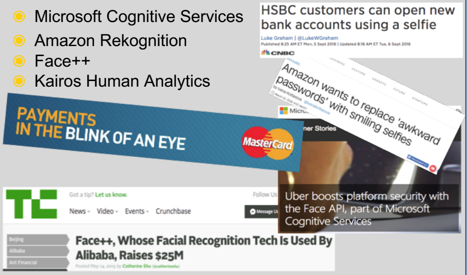
Georgia Tech | Institute for Information Security & Privacy

NDSS '18 SYMPOSIUM

SMILE, AND YOU ARE AUTHENTICATED

Face Verification Cloud Services

- Microsoft Cognitive Services
- Amazon Rekognition
- Face++
- Kairos Human Analytics



HSBC customers can open new bank accounts using a selfie

Luke Graham | @LukeWGraham

Published 8:25 AM ET Mon, 5 Sept 2016 | Updated 8:18 AM ET Tue, 6 Sept 2016

CNBC

Amazon wants to replace 'awkward passwords' with smiling selfies

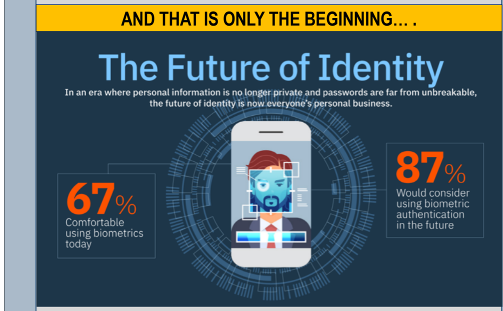
PAYMENTS IN THE BLINK OF AN EYE

MasterCard

Uber boosts platform security with the Face API, part of Microsoft Cognitive Services

Face++, Whose Facial Recognition Tech Is Used By Alibaba, Raises $25M

AND THAT IS ONLY THE BEGINNING… .



The Future of Identity

In an era where personal information is no longer private and passwords are far from unbreakable, the future of identity is now everyone's personal business.

67% Comfortable using biometrics today
87% Would consider using biometric authentication in the future

Image Credit: IBM Future of Identity Study

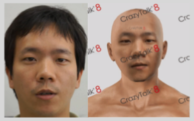
UNFORTUNATELY… CRAZYTALK HAPPENED…

The free sample of the tool CrazyTalk can create cartoon version of a person and defeat all tested systems….

- 100% impersonation against Face API (MS), Face++ (Alipay)
- 90% impersonation against Amazon Rekognition

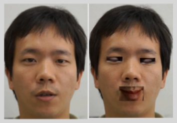
Also defeats existing liveness detection

- You can make the cartoon smile, blink, nod, talk whenever you want



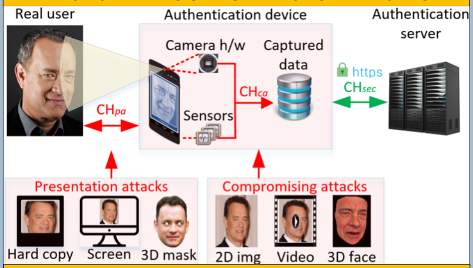
Genuine Spoofed

MS Face API	: 68% Similarity
Amazon Rec	: 74% Similarity
Face++	: 88% Similarity
Kairos	: 75% Similarity

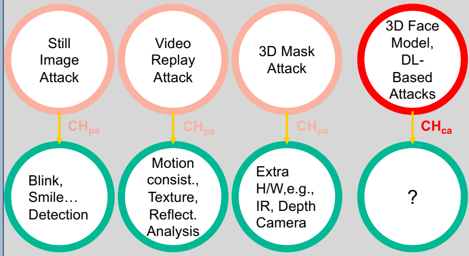


Genuine	Spoofed
Smile: 0.001	**Smile:** 0.421

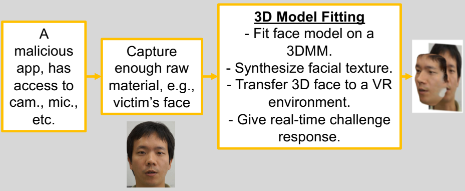
ATTACK CHANNELS OF BIOMETRIC AUTHENTICATION



ADVERSARIAL MODELS vs DEFENSE SYSTEMS



COMPROMISING ATTACK EXAMPLE



A malicious app, has access to cam., mic., etc. → Capture enough raw material, e.g., victim's face → **3D Model Fitting**

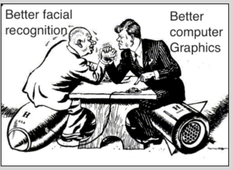
- Fit face model on a 3DMM.
- Synthesize facial texture.
- Transfer 3D face to a VR environment.
- Give real-time challenge response.

THREAT MODEL

Automated compromising attacks.

- Camera, microphone and device kernel are compromised.
- No form of attestation.
- Known client-server protocol.
- State-of-the art synthesizers and Captcha breaking tools.
- Authentication server is NOT compromised.

ENDLESS ARMS RACE vs A MORE FUNDAMENTAL APPROACH?



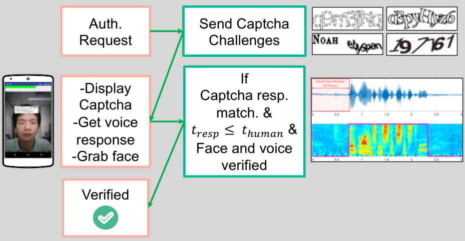
IDEA: Base our solution on a known hard problem

CHALLENGE: Prove you are the real user by reading the answer to the CAPTCHA in front of the camera please.

Computer graphics will NOT help since you can NOT generate the right video without solving the CAPTCHA.

OUR APPROACH: rtCAPTCHA

Send randomized challenges as CAPTCHA

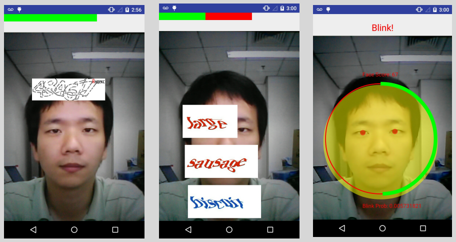


Auth. Request
Send Captcha Challenges
-Display Captcha -Get voice response -Grab face
If Captcha resp. match. & $t_{resp} \leq t_{human}$ & Face and voice verified
Verified

USER STUDY

Challenges

- Plaintext – Numeric and Phrases
- Numeric Captchas – reCaptcha, Ebay, Yandex
- Animated Phrase Captchas – reCaptcha
- Blink/Smile



ACCURACY ANALYSIS

Challenge	Accuracy (%) (1 trial)	Accuracy (%) (2 trials)	Response Time (seconds)
Plain-text	90.3	100	0.77
Captcha	88.8	98.4	0.93
Smile/Blink	85.5	100	5.01

SECURITY ANALYSIS

$\mathbf{Hum_{aud}}$: Users in our user study.

$\mathbf{Atc_{typ}}$: Man-powered Captcha solving services.

$\mathbf{Atc_{ocr}}$: OCR-based Captcha decoding services.

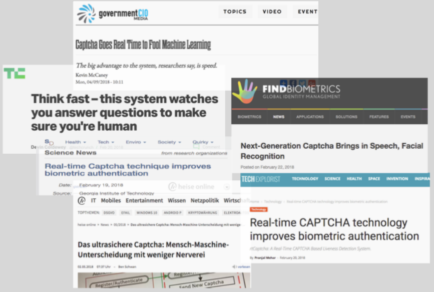
$\mathbf{Atc_{best}}$: State-of-the art Captcha breaking tool.

Captcha Sample	Captcha Scheme	Recognition Accuracy (%)			
		Hum_{aud}	Atc_{typ}	Atc_{ocr}	Atc_{best}
	$reCaptcha_{numeric}$	87.1	96.7	0	77.2
	$Ebay_{numeric}$	94.1	100	0	58.8
	$Yandex_{numeric}$	87.7	96.7	0	2.2
	$reCaptcha_{phrase}$	88.0	91.5	0	N/A

Captcha Sample	Captcha Scheme	Response Time (seconds)			
		Hum_{aud}	Atc_{typ}	Atc_{ocr}	Atc_{best}
	$reCaptcha_{numeric}$	0.90	22.11	2.98	10.27
	$Ebay_{numeric}$	0.73	12.33	2.79	5.98
	$Yandex_{numeric}$	0.89	15.05	3.30	15.50
	$reCaptcha_{phrase}$	1.02	20.88	3.03	N/A

CONCLUSIONS

- Smile/blink etc. detection is weak against spoofing.
- rtCaptcha: Audio/image analysis → CAPTCHA
- rtCaptcha: Very limited time to;
  - Break Captcha
  - Synthesize voice/face of the victim.
- Limitation: rtCaptcha needs audible response, which could NOT be usable in certain environments.



governmentCIO MEDIA

Captcha Goes Real Time to Fool Machine Learning

The big advantage to the system, researchers say, is speed.

Kevin McCaney

Mon, 04/09/2018 - 10:11

Think fast – this system watches you answer questions to make sure you're human

Science News

Real-time Captcha technique improves biometric authentication

Date: February 19, 2018

Source: Georgia Institute of Technology

FINDBIOMETRICS GLOBAL IDENTITY MANAGEMENT

Next-Generation Captcha Brings in Speech, Facial Recognition

Posted on February 22, 2018

TECH EXPLORIST

Real-time CAPTCHA technology improves biometric authentication

heise online

Das ultrasichere Captcha: Mensch-Maschine-Unterscheidung mit weniger Nerverei

POSTER TEMPLATE BY: www.PosterPresentations.com