

COMPUTER SECURITY

ACCESS CONTROL
(AUTHENTICATION)

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

Access Control

- Issues concerning access of system resources
- Two big part of access control:
 - Authentication
 - Authorization



Authentication

Who Are You?



PIN & Fingerprint



Proximity Card



Key Fob

Authentication Method

- Human can be authenticated based on any combination:
 - Something you know
 - Passwords/PINs
 - Something you have
 - ATM Cards, Access Cards
 - Something you are
 - Retina, Fingerprints (biometrics)

Password

- Most basic, easy and commonly used security protection
- But also often misused by many users
 - Using easy to guess password
 - Using short password
 - Never changed password regularly
 - Password sharing
- Prone to many attacks
 - Passive/active online attack
 - Offline attack
 - Non-technical attack



Trivia Quiz

Who uses the same passwords
for Email, Facebook, Twitter,
and any other web site?

I bet more than 50% of class :)

Close to 1% of all accounts at RockYou used 123456 as their passwords. That's 290,731 accounts out of 32M.

The remainder of the top 20 are as follows:

Rank	Password	Number of Users with Password
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

<http://www.nytimes.com/2010/01/21/technology/21password.html>

<http://www.itwire.com/business-it-news/security/30654-what-is-the-most-popular-password>

Also Read:

<http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time>

Why Passwords?

- Costs

- Passwords are free
- Easy to generate/regenerate
- Smartcards and biometrics devices cost money



- Convenience

- Easy to set up and maintain for administrator
- No need to bring extra devices for user



Password Generator

- Helps you to generate secure password
 - <http://www.pctools.com/guides/password/>
 - <http://www.goodpassword.com/>
 - <http://strongpasswordgenerator.com/>
 - <http://tools.arantius.com/password>
 - <http://www.thebitmill.com/tools/password.html>
- Helps you to test your password
 - <http://www.passwordmeter.com/>
 - <http://www.yetanotherpasswordmeter.com/>

Randomly Generated Keys

- Solves problem with passwords
- Unfortunately, not many people like it (hard to remember)
- Example:
 - Using 64-bit cryptographic key $\rightarrow 2^{64}$ possible key
 - Using 8 characters long with 256 possibility for each character $\rightarrow 256^8 \sim 2^{64}$ **BUT which one do you prefer?**
 - computer
 - kf&Yw!a[
 - Using alphabet characters only will reduce it to 26^8 possibilities

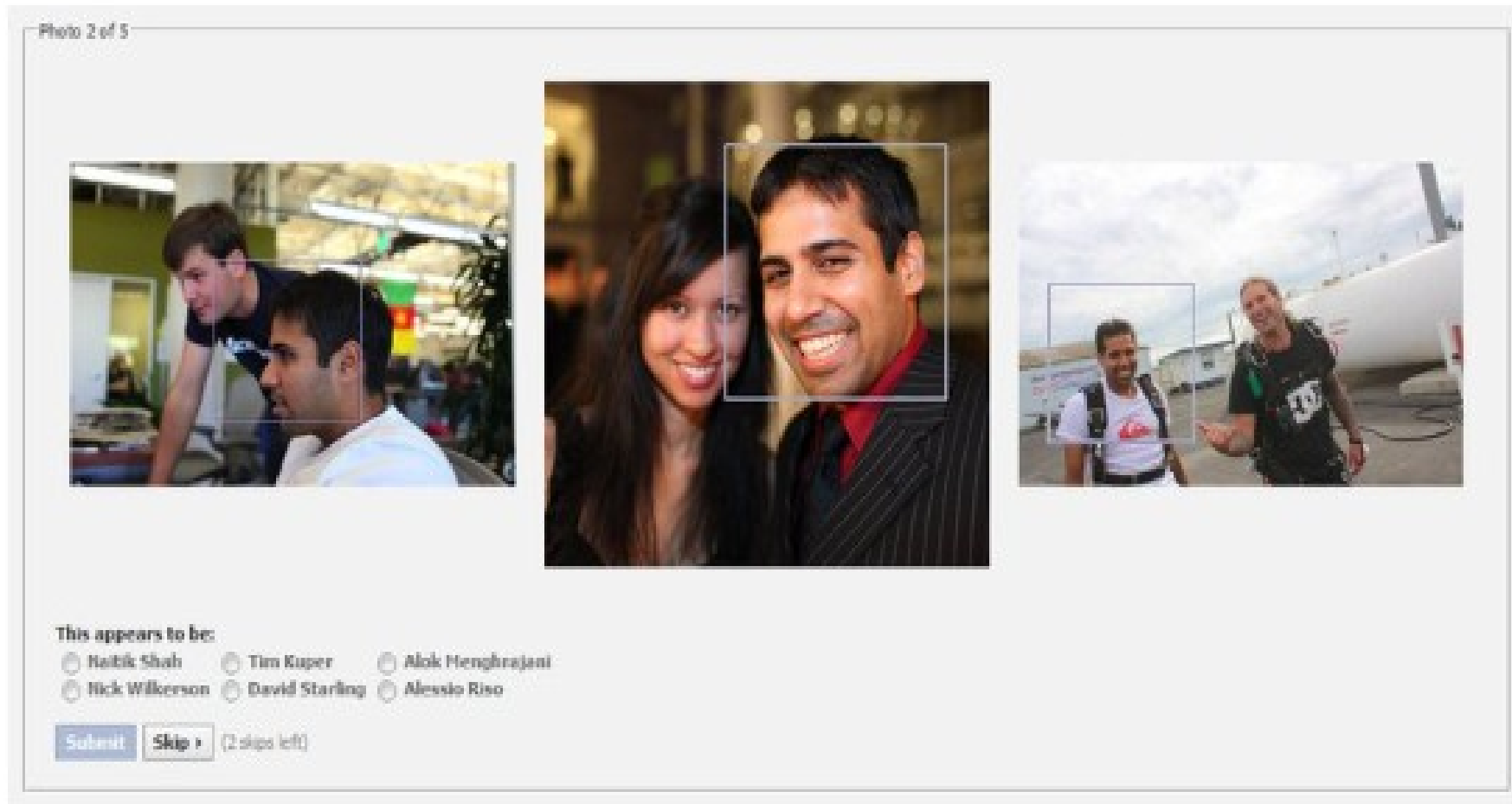
Password Combinations

- Formula = (possible of key space)ⁿ
 - n = length of password
- Example:
 - Length = 8
 - Alphabet only = $26^8 = 208.827.064.576$
 - Alphanumeric case-insensitive = $36^8 = 2.821.109.907.456$
 - Alphanumeric case-sensitive = $62^8 = 2.18340106 \times 10^{14}$

Password Issues

- Too many passwords to remember
 - Results in password reuse
- Failure to change default passwords
- Social engineering
- Bugs, keystroke logging, spyware, etc.

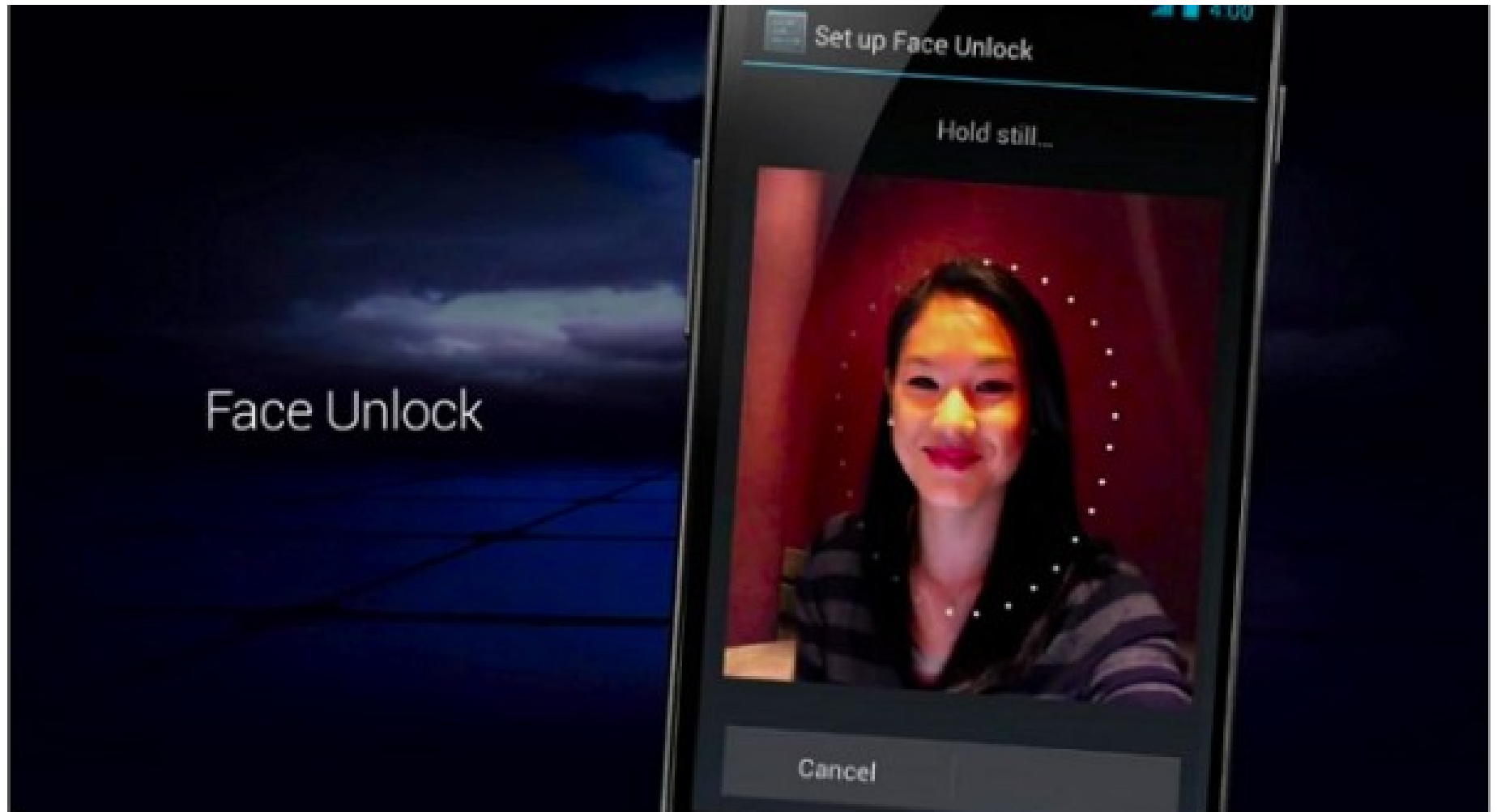
Social Authentication @ Facebook



Social authentication

<http://blog.facebook.com/blog.php?post=486790652130>

Face Unlock on Android



Smart Cards

A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data

This data can be used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use

A smart card contains more information than a magnetic strip card and can be programmed for different applications



Security Token

According to the search security definition, “A security token is a small hardware device that the owner carries to authorize access to a network service”



Security tokens provide an extra level of assurance through a method known as two-factor authentication:

- The user has a personal identification number (PIN) that authorizes them as the owner of that particular device
- The device then displays a number that uniquely identifies the user to the service, allowing them to log in





Biometrics

- **“You are your key”** ~ Schneier
- Examples
 - Fingerprint
 - Handwritten signature
 - Facial recognition
 - Speech recognition
 - Gait (walking) recognition
 - “Digital doggie” (odor recognition)
 - Many more!

Why Biometrics

- Biometrics seen as desirable replacement for passwords
- Cheap and reliable biometrics needed
- Today, a very active area of research
- Biometrics are used in security today
 - Thumbprint mouse
 - Palm print for secure entry
 - Fingerprint to unlock car door, etc.
- But biometrics not too popular
 - Has not lived up to its promise (yet)

Biometric Devices

Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and a location for the data to be analyzed; for instance a database that stores the biometric data for comparison with previous records

Methods used by biometric devices for access control are:

- Fingerprints
- Face scan
- Iris scan
- Voice recognition



Biometric Identification Techniques

Fingerprinting

- Ridges and furrows on the surface of a finger are used to identify a person, which are unique



Iris Scanning

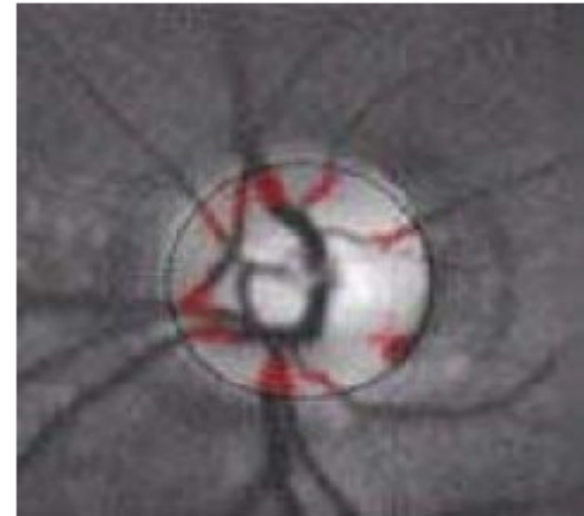
- Analyzes the colored part of the eye suspended behind the cornea



Biometric Identification Techniques

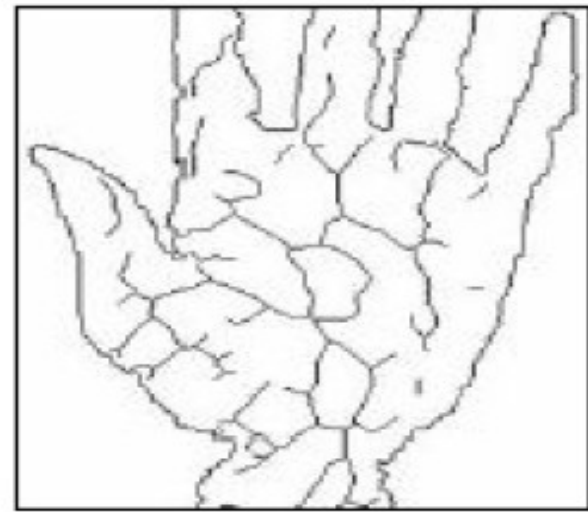
Retinal scanning

- Identifies a person by analyzing the layer of blood vessels at the back of the eye



Vein Structure

- Thickness and location of veins are analyzed to identify person



Biometrics Challenges

Fingerprints can be faked with ease



Face recognition systems can be tricked by masquerade techniques

Signature recognition and hand geometry face the common problem of matching the patterns from a large database which might lead to higher number of false positives and false negatives

Retinal scan can hinder accuracy if the user does not focus on a given point for scan. Iris scan machines are very expensive

Some users object to vascular pattern technology that uses infrared light

Voice dynamics is prone to inaccuracy as it relies on the production of a "voice template" that is compared with a spoken phrase

Biometrics Ideal

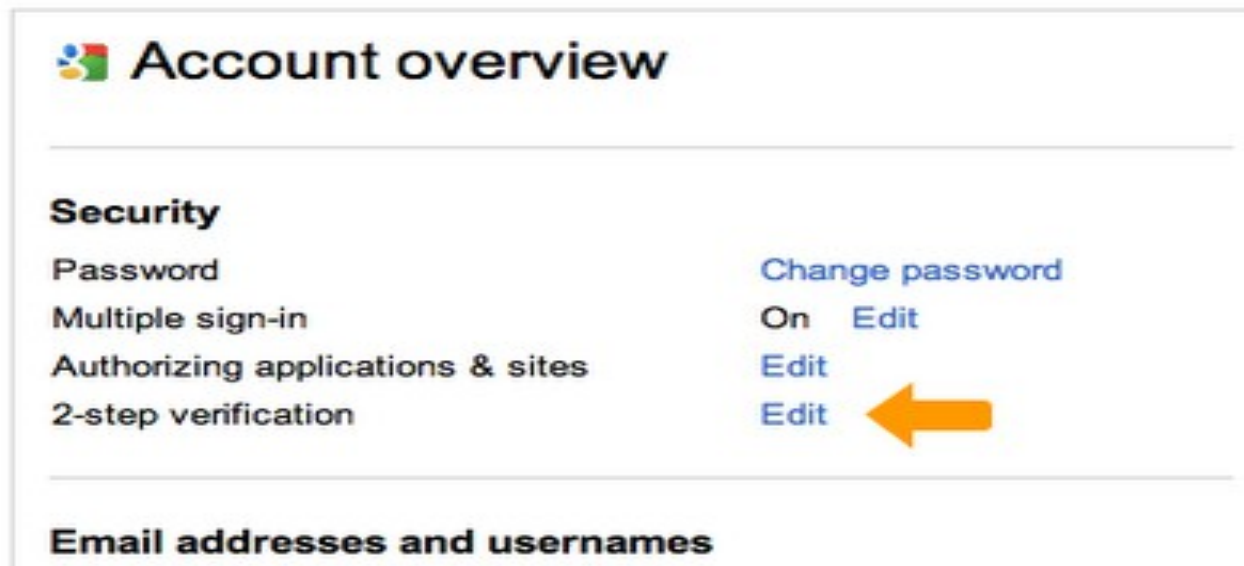
- Universal: applicable to everyone
- Distinguishing: 100% certainty
- Permanent: characteristics should never change
- Collectable: easy to collect without harming the subject
- Reliable, Robust, and User Friendly: not only in labs

Which technology qualified all above requirements?

Two Factor Authentication

- Requires two out of three authentications
- Example: Password Generator, ATM Cards
 - Something you have: password generator device, ATM Card
 - Something you know: PIN
- Other example: Face recognition on laptop
 - Something you have: web camera on laptop
 - Something you are: your own face

Google Two Factor Authentication



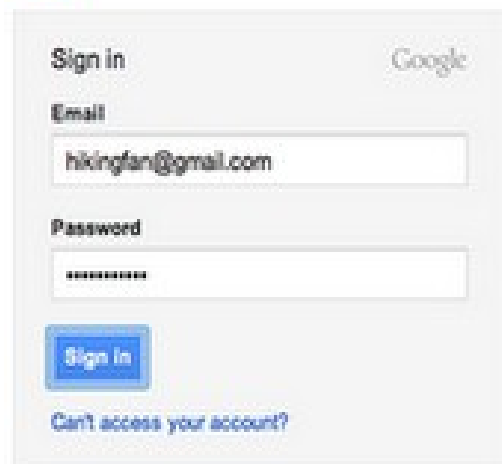
 **Account overview**

Security

Password	Change password
Multiple sign-in	On Edit
Authorizing applications & sites	Edit
2-step verification	Edit 

Email addresses and usernames

1.



Sign in Google

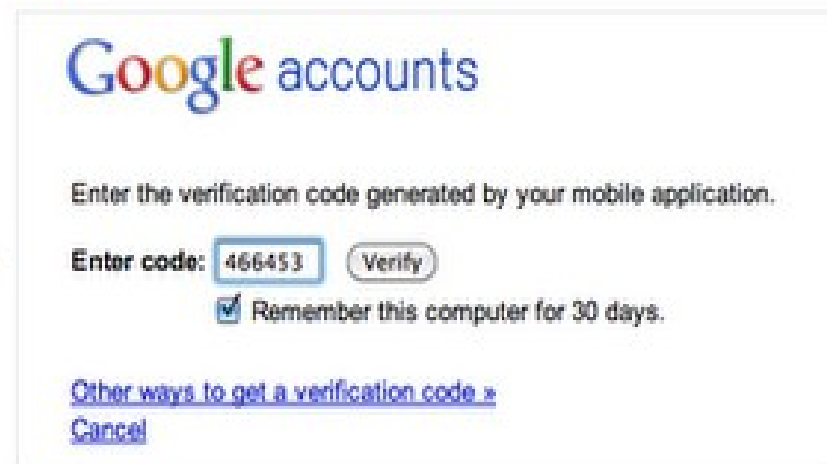
Email

Password

[Sign in](#)

[Can't access your account?](#)

2.



Google accounts

Enter the verification code generated by your mobile application.

Enter code: [Verify](#)

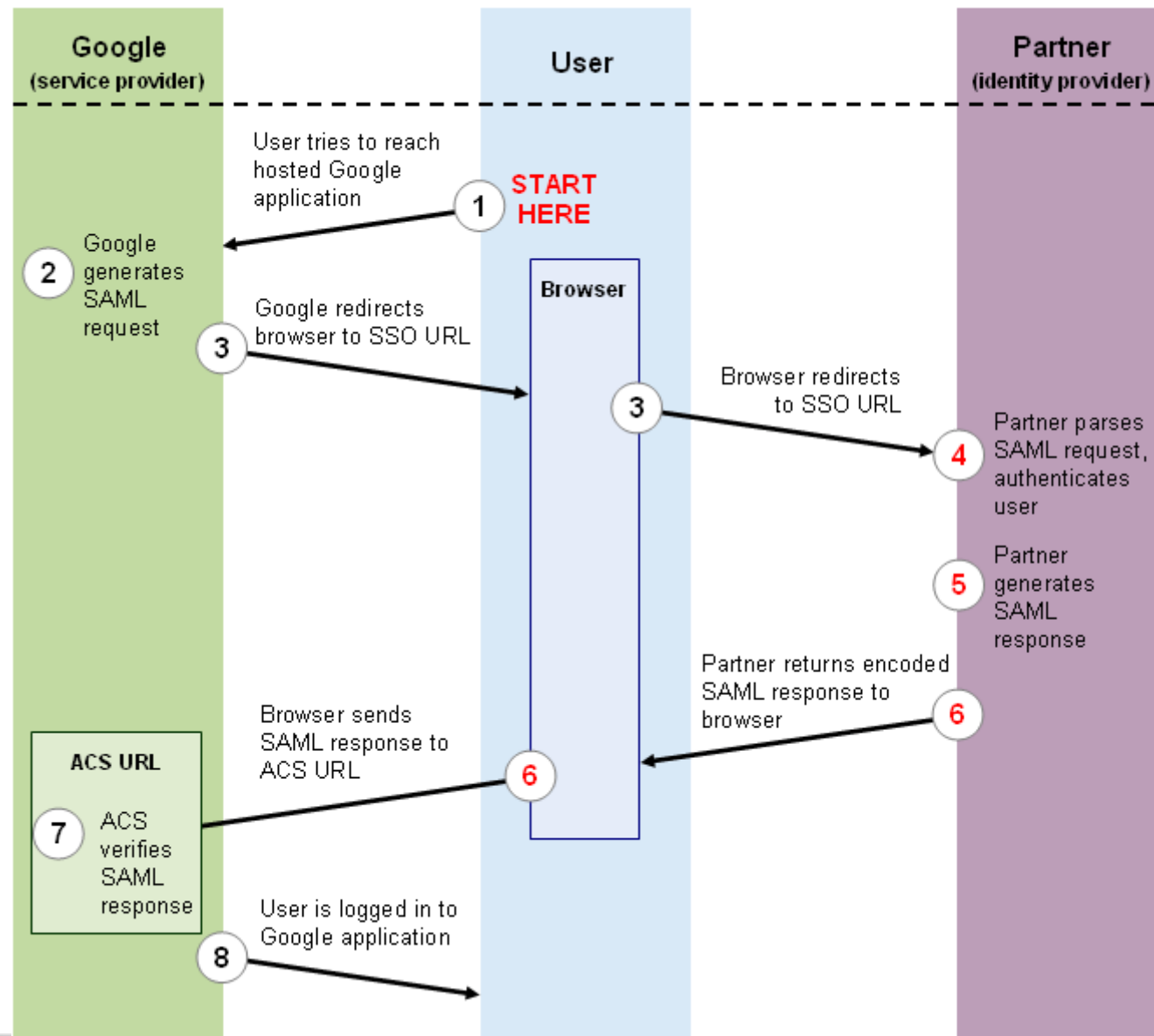
☒ Remember this computer for 30 days.

[Other ways to get a verification code »](#)

[Cancel](#)

Single Sign-On

SAML Transaction Steps



Single Sign-On

- Kerberos
- Active-Directory (Windows)
- PAM (Linux)
- Smart Card
- OTP Token