Identity and authentication

Introduction

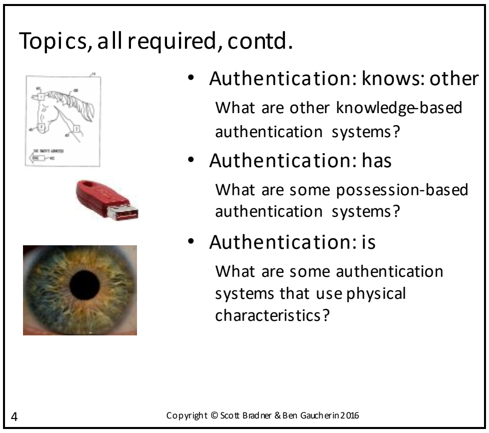
CSCI E 45b: The Cyber World – part B

Introduction: learning goals

- Understand what identity and authentication are and how they relate
- Understand the types of authentication approaches
- Understand the strengths and weakness of the approaches
- Understand how different approaches can be combined for better security

Topics, all required

- Identity
  - What is an identity?
  - How are identities used?
- Authentication
  - What is authentication used for?
  - What are the basic factors used in authentication systems?
- Authentication: knows: passwords
  - What are the issues with password-based systems?
  - How can the issues be minimized?



Topics, all required, contd.

- Authentication: knows: other

  What are other knowledge-based authentication systems?

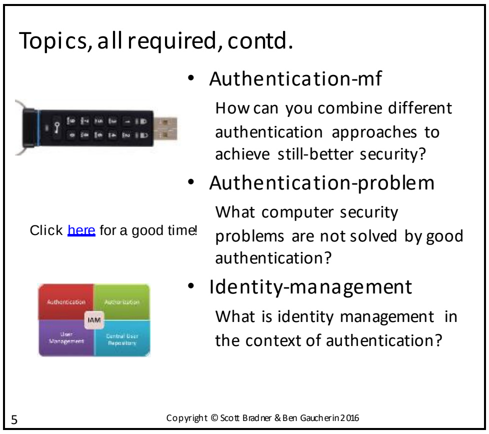
- Authentication: has

  What are some possession-based authentication systems?

- Authentication: is

  What are some authentication systems that use physical characteristics?

4 Copyright © Scott Bradner & Ben Gaucherin 2016



Topics, all required, contd.

Click here for a good time!

- Authentication-mf

  How can you combine different authentication approaches to achieve still-better security?

- Authentication-problem

  What computer security problems are not solved by good authentication?

- Identity-management

  What is identity management in the context of authentication?

5 Copyright © Scott Bradner & Ben Gaucherin 2016

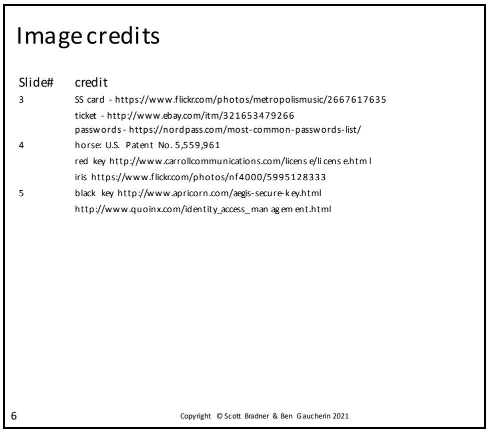


Image credits

Slide#	credit
3	SS card - https://www.flickr.com/photos/metropolismusic/2667617635
	ticket - http://www.ebay.com/itm/321653479266
	passwords - https://nordpass.com/most-common-passwords-list/
4	horse: U.S. Patent No. 5,559,961
	red key http://www.carrollcommunications.com/license/license.html
	iris https://www.flickr.com/photos/nf4000/5995128333
5	black key http://www.apricorn.com/aegis-secure-key.html
	http://www.quoinx.com/identity_access_management.html

6 Copyright © Scott Bradner & Ben Gaucherin 2021

Identity and authentication

Identity

CSCI E 45b: The Cyber World – part B

1

Identity

Merriam-Webster	- *“who someone is: the name of a person”* - *“the qualities, beliefs, etc., that make a particular person or group different from others”*
The free dictionary	- *“the individual characteristics by which a person or thing is recognized”*

2

An identity

- Uniquely specify an individual person

  e.g., name, username, ID number, set of characteristics
- An identification is usually created within a specific context

  e.g.,

  User account names

  Passport numbers

  Driver’s license numbers

  Social Security numbers

3

An identity, contd.

Continuity of identification without an actual identification

- Sometimes use of an identification is extended beyond the original context
  e.g., Social Security numbers
- Note that a context could be 'the same person I talked to yesterday' with no binding to a known specific person
  See Purpose Built Keys (PBK)

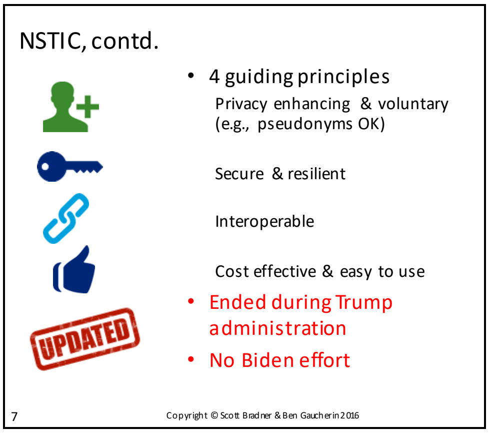
An identity, contd.

- Often, ID used without the person directly involved
  e.g., employer sending earnings information to tax man
- ID used to define to whom information applies
- ID only useful if ID issued by a trusted party to a unique individual
- Real ID implies specific verification procedures

NSTIC

NSTIC

- National Strategy for Trusted Identities in Cyberspace (NSTIC)
  Helping individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation
- U.S. government effort
- Bless private identity providers – e.g. Harvard



NSTIC, contd.

- 4 guiding principles
  - Privacy enhancing & voluntary (e.g., pseudonyms OK)
  - Secure & resilient
  - Interoperable
  - Cost effective & easy to use
- Ended during Trump administration
- No Biden effort

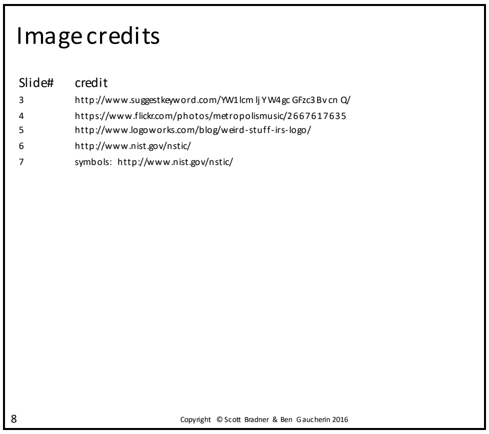


Image credits

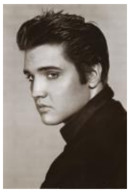
Slide#	credit
3	http://www.suggestkeyword.com/YW1lcmljYW4gcGFzc3BvcnQ/
4	https://www.flickr.com/photos/metropolismusic/2667617635
5	http://www.logoworks.com/blog/weird-stuff-irs-logo/
6	http://www.nist.gov/nstic/
7	symbols: http://www.nist.gov/nstic/

Identity and authentication

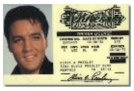
Authentication

CSCI E 45b: The Cyber World – part B

Authentication



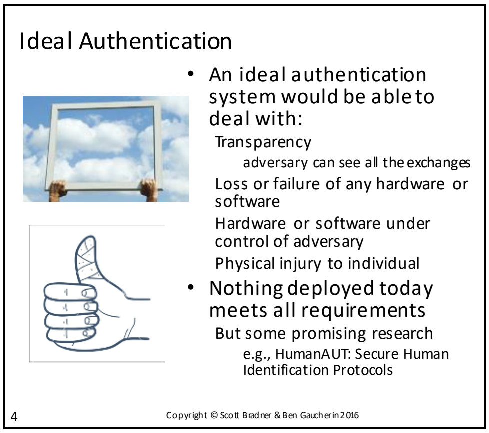
Elvis Presley



- Authentication
  - Bind a physical person to an identification
    - Whether you know the person's identity or not
- When a person needs to authenticate
  - They need to provide the ID value
    - Account name, ID number, driver's license number, etc.
    - Note that personal names are ambiguous IDs in many cases
  - And provide a verifier that they are the person who is specified by that ID value
    - e.g., physical presence and picture ID, password, …

Authentication by possession or knowledge

- In some cases, knowledge of the ID itself is seen as authenticating
  - e.g., bank's use of SSNs
    - The banks believe SSNs are secret
- In some cases you can authenticate without identifying
  - e.g., movie ticket
    - Authenticate that you are a member of the group of people who paid to see the movie, but no identity is used (e.g., name)

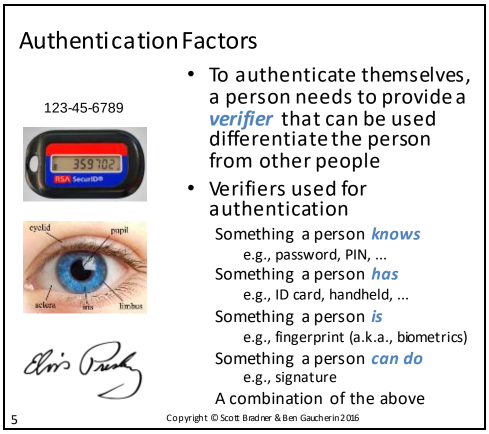


Ideal Authentication

- An ideal authentication system would be able to deal with:
  - Transparency
    - adversary can see all the exchanges
  - Loss or failure of any hardware or software
  - Hardware or software under control of adversary
  - Physical injury to individual
- Nothing deployed today meets all requirements
  - But some promising research
    - e.g., HumanAUT: Secure Human Identification Protocols

4

Copyright © Scott Bradner & Ben Gaucherin 2016



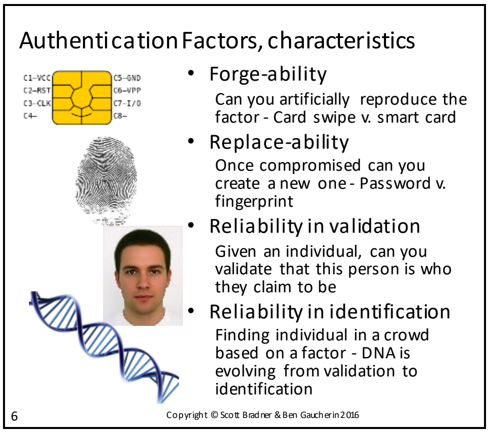
123-45-6789
359702
RSA SecurID
eyelid
pupil
sclera
iris
limbus

Authentication Factors

- To authenticate themselves, a person needs to provide a ***verifier*** that can be used differentiate the person from other people
- Verifiers used for authentication
  - Something a person ***knows***
    - e.g., password, PIN, …
  - Something a person ***has***
    - e.g., ID card, handheld, …
  - Something a person ***is***
    - e.g., fingerprint (a.k.a., biometrics)
  - Something a person ***can do***
    - e.g., signature
  - A combination of the above

5

Copyright © Scott Bradner & Ben Gaucherin 2016



C1–VCC
C2–RST
C3–CLK
C4–
C5–GND
C6–VPP
C7–I/O
C8–

Authentication Factors, characteristics

- Forge-ability
  - Can you artificially reproduce the factor - Card swipe v. smart card
- Replace-ability
  - Once compromised can you create a new one - Password v. fingerprint
- Reliability in validation
  - Given an individual, can you validate that this person is who they claim to be
- Reliability in identification
  - Finding individual in a crowd based on a factor - DNA is evolving from validation to identification

6

Copyright © Scott Bradner & Ben Gaucherin 2016

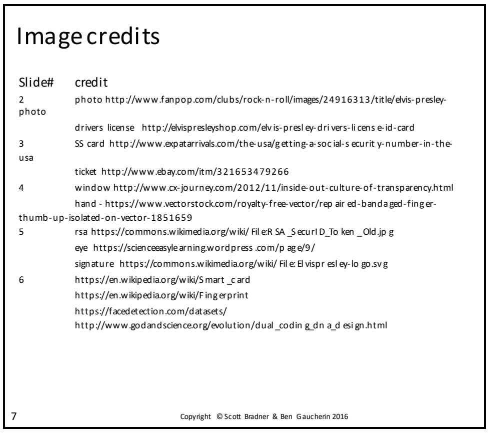


Image credits

Slide#	credit
2	photo http://www.fanpop.com/clubs/rock-n-roll/images/24916313/title/elvis-presley-photo
	drivers license http://elvispresleyshop.com/elvis-presley-drivers-license-id-card
3	SS card http://www.expatarrivals.com/the-usa/getting-a-social-security-number-in-the-usa
	ticket http://www.ebay.com/itm/321653479266
4	window http://www.cx-journey.com/2012/11/inside-out-culture-of-transparency.html
	hand - https://www.vectorstock.com/royalty-free-vector/repaired-bandaged-finger-thumb-up-isolated-on-vector-1851659
5	rsa https://commons.wikimedia.org/wiki/File:RSA_SecurID_Token_Old.jpg
	eye https://scienceeasylearning.wordpress.com/page/9/
	signature https://commons.wikimedia.org/wiki/File:Elvispresley-logo.svg
6	https://en.wikipedia.org/wiki/Smart_card
	https://en.wikipedia.org/wiki/Fingerprint
	https://facedetection.com/datasets/
	http://www.godandscience.org/evolution/dual_coding_dna_design.html

Identity and authentication

Authentication – knows - passwords

CSCI E 45b: The Cyber World – part B

Something a Person ***Knows***

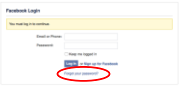
Here's 2022's worst passwords don't use any of these

123456
admin
12345678
123456789
1234
12345
password
123
Aa123456
1234567890

UPDATED

- e.g., password
- **Ideal**: this is something that is ONLY known by a single individual
  - e.g., a password which cannot be retrieved by a system administrator
  - i.e, store a hash of the password, not the password itself

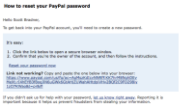
Something a Person ***Knows***, contd.


Facebook Login

You must log in to continue.

Email or Phone:

Password:


How to reset your PayPal password

Hello Scott Bradner,

To get back into your PayPal account, you'll need to create a new password.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Reset your password now

Link not working? Copy and paste the one below into your browser:
[illegible]

If you didn't ask us for help with your password, let us know right away. Reporting it is important because it helps us prevent fraudsters from stealing your information.

- Systems that can tell you your password if you forget it do not meet this requirement
  - Since the password must be stored in a way that it can be retrieved to be able to return it to you
  - Systems that send you a temporary password or URL to enter in a new one may be OK
    - Or might not be - depends on design

Password Failure Mode

I am

you

- If I know your account name and password, then (to the computer) I am you
- The computer cannot prevent me from doing anything you are empowered to do
  - While making it look like you did it
- Therefore, if the system administrator can know your password, they can act as you
  - And you cannot prove they did so

Passwords

- Most common way of authentication
  - Far too common, many new requirements
    - Lots of devices
      - Multiple computers, handhelds, phones, ...
    - Web sites that need authentication to provide service
      - wsj.com, united.com, ...
    - Web sites that insist that you set up an account before you can buy something
      - Too many to list
- Often not stored securely
  - Use bcrypt

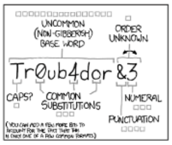
Passwords, contd.

- Should use different passwords for different places
  - Unless no private information and no stored ability to purchase anything at any site
    - Need to worry about site with **weakest security**
    - Not all sites ask for password over secure channel

UPDATED

FedEx has updated its home page to use https/SSL

Passwords, contd.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

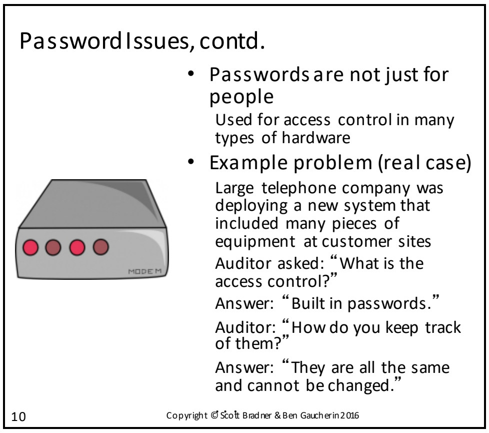
- Poor consideration of human factors
  - Strict rules on password creation can be hard for many users
    - Or cause the use of passwords that get written down
  - Assigned (and unchangeable) passwords
- Too many are too easy to guess or too easy to forget

Password Issues

- How to manage passwords
  - Ideal – use different passwords everywhere
    - Need to remember many passwords
  - Can use password management system
    - One well-chosen & guarded password to enable many individual (maybe random) passwords

Password Issues, contd.

- What to do with “important” passwords
  - How to protect against person leaving or getting “truck fade”
    - Escrow in access controlled safe? - log access
  - e.g., admin password to very secure server
    - Password, kept in safe, changed after each use, relocked in safe
  - Restrict use
    - e.g., require “sudo” or “run as administrator” rather than login as root

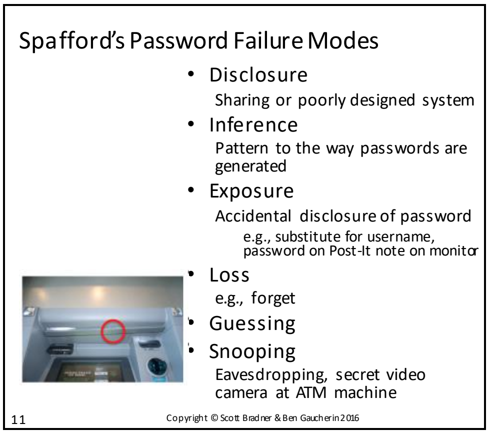


Password Issues, contd.

- Passwords are not just for people
  - Used for access control in many types of hardware
- Example problem (real case)
  - Large telephone company was deploying a new system that included many pieces of equipment at customer sites
  - Auditor asked: "What is the access control?"
  - Answer: "Built in passwords."
  - Auditor: "How do you keep track of them?"
  - Answer: "They are all the same and cannot be changed."

10

Copyright © Scott Bradner & Ben Gaucherin 2016

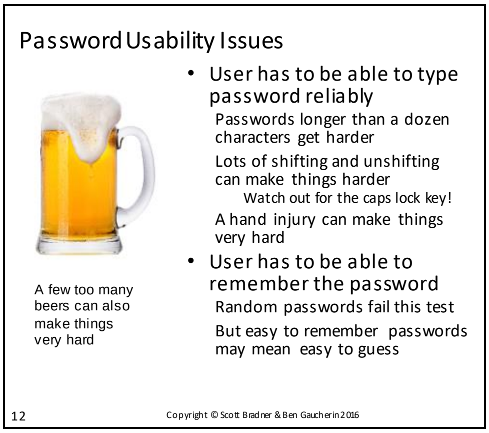


Spafford's Password Failure Modes

- Disclosure
  - Sharing or poorly designed system
- Inference
  - Pattern to the way passwords are generated
- Exposure
  - Accidental disclosure of password
    - e.g., substitute for username, password on Post-It note on monitor
- Loss
  - e.g., forget
- Guessing
- Snooping
  - Eavesdropping, secret video camera at ATM machine

11

Copyright © Scott Bradner & Ben Gaucherin 2016



Password Usability Issues

- User has to be able to type password reliably
  - Passwords longer than a dozen characters get harder
  - Lots of shifting and unshifting can make things harder
    - Watch out for the caps lock key!
  - A hand injury can make things very hard
- User has to be able to remember the password
  - Random passwords fail this test
  - But easy to remember passwords may mean easy to guess

A few too many beers can also make things very hard

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Harvard's Password Rules

UPDATED

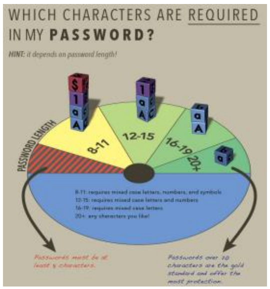
~~xxxxxxxxx~~

~~12345aaaa~~

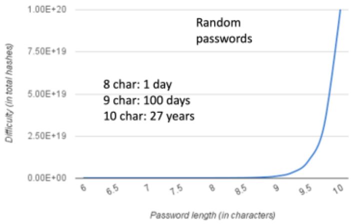
- Must be a secret between user and system
  - And never stored in a retrievable way
- Must be long or "complex"
  - no rules if passphrase
  - 1. > 10 characters
  - 2. Include at least one character from at least 3 of the following:
    - uppercase letter, lowercase letter, number, special character

Stanford University password policy

- The longer the password, the fewer the requirements


WHICH CHARACTERS ARE REQUIRED IN MY PASSWORD?
HINT: it depends on password length!
PASSWORD LENGTH
8-11
12-15
16-19
20+
$
1
a
A
8-11: requires mixed case letters, numbers, and symbols
12-15: requires mixed case letters and numbers
16-19: requires mixed case letters
20+: any characters you like!
Passwords must be at least 8 characters.
Passwords over 20 characters are the gold standard and offer the most protection.

Password Length vs. Difficulty

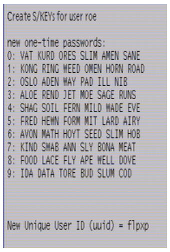


Random passwords

8 char: 1 day
9 char: 100 days
10 char: 27 years

Robert David Graham

One-Time Passwords



```
Create S/KEYs for user roe

new one-time passwords:
0: VAT KURD ORES SLIM AMEN SANE
1: KONG RING WEED OMEN HORN ROAD
2: OSLO ADEN WAY PAD ILL NIB
3: ALOE REND JET MOE SAGE RUNS
4: SHAG SOIL FERN MILD WADE EVE
5: FRED HEWN FORM MIT LARD AIRY
6: AVON MATH HOYT SEED SLIM HOB
7: KIND SWAB ANN SLY BONA MEAT
8: FOOD LACE FLY APE WELL DOVE
9: IDA DATA TORE BUD SLUM COD


New Unique User ID (uuid) = flpxp
```

- Use a new password each time
- Removes most of Spafford's risks

  Interference and loss of password generator are still issues
- Paper-based

  User gets list of use-once passwords, use & cross off

  system has same list

  e.g., S/KEY
- Electronic

  Get password for next login when successfully logged in

Image credits

2	https://www.makeuseof.com/nordpass-reveals-the-worst-passwords-of-2021-is-yours-one-of-them/
3	facebook https://www.facebook.com/login.php?next=https%3A%2F%2Fwww.facebook.com%2Fhome.php
	paypal
4	blank face https://www.pinterest.com/pin/376824693792389573/
5	https://www.ashleymadison.com/
6	bank http://classroomclipart.com/clipart-search/page-9/all-or/piggy%20bank/
	hospital http://elderlawblogtn.com/2013/08
	office http://bestarchitecturalbuilding.blogspot.com/2013/09/clipart-gallery-buildings-temples.html
	food http://www.fotosearch.de/IMZ244/rga0056/
7	https://xkcd.com/936/
8	http://www.hddfiresafe.com/index.php/fireking-three-hour-data-safe-dm4420-3.html
9	http://jpchrome.com/Tools/Portfolio/frontend/item.asp?type=48&size=0&lngDisplay=0&jPageNumber=14&strMetaTag=
10	http://www.vectors4all.net/vectors/dsl-cable-modem-clip-art

Image credits

Slide#	credit
11	https://oag.ca.gov/system/files/attachments/press_releases/camera%20ATM_2216.JPG
12	http://www.thriveswla.com/places-faces/bottoms-up-for-the-lake-charles-winter-beer-fest
14	http://arstechnica.com/security/2014/04/stanfords-password-policy-shuns-one-size-fits-all-security/
15	http://blog.erratasec.com/2011/06/password-cracking-mining-and-gpus.html
16	http://docs.oracle.com/cd/E19957-01/805-7688/z40003a31007698/index.html

Identity and authentication

Authentication – knows – other

CSCI E 45b: The Cyber World – part B

Graphical Passwords

- Replace character strings with graphical information
  - Different approaches
- Advantages
  - Hard to write down
  - Hard to share your password
  - Hard to do dictionary attacks

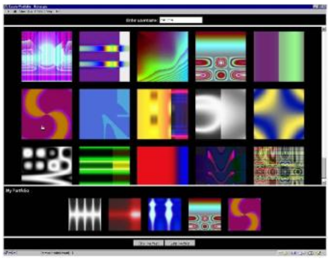
Faces

- Learn *N* faces
- Pick out from matrix
  - Presented one 3x3 matrix at a time
- Issue: Prosopagnosia
  - Face-blindness

Select Pictures

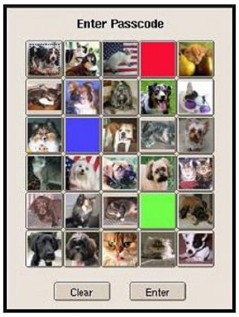
- Pick *N* pictures from matrix

  Can use generated pictures (not photos) to minimize bias



Dhamija & Perrig

Select Pictures, contd.

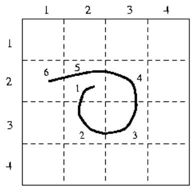


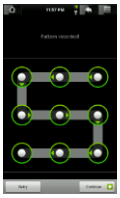
NIST

Draw Patterns

- e.g., Draw-a-Secret (DAS)
- Draw a pattern on a grid

  Pattern and direction of line(s) used as password





Blonder Picture Passwords

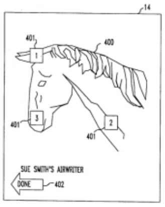


Figure 4 from U.S. Patent No. 5,559,961

- Patented by Greg Blonder (patent #5,559,961)
  - Click on a sequence of locations within a picture

Reverse Turing Test

- Aim is to block computer generated guessing
- Present distorted images of text & ask user to type them
  - CAPTCHA
  - **C**ompletely
  - **A**utomated
  - **P**ublic
  - **T**uring test to tell
  - **C**omputers and
  - **H**umans
  - **A**part
  - Verify that there is a human present
    - But is it the right human?

Fighting Guessing Attacks

Mr.Vigilant

- Aim: make it hard for automated on-line guessing attacks to work
  - Off-line attack on leaked password files is a different issue
  - Not easy to block guessing-with-knowledge attacks
    - Where attacker knows a lot about you & guesses what you might use
- Automated guessing can do 100's of thousands of guesses per day
  - Attackers try guessed passwords in probability order

Fighting Guessing Attacks, contd.

LOPHTCRACK

ophcrack

John the Ripper

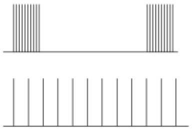
- Sysadmin can run password cracker on passwords

  To see if anyone is using a weak password

  Or to break in

10

Fighting Guessing Attacks, contd.



- Defense against remote guessers

  Automatic lockout - disable account after *N* failed login attempts

  Can automatically re-enable after some period of time

  e.g., 30 minutes

  Can require intervention by support personnel

  Provides little additional protection, can be very disruptive

- Not a defense against rogue sysadmins grabbing password files

11

Fighting Guessing Attacks, contd.

Syslog Messages
Workstations
Applications
Servers
GFI EventsManager
Devices

- In any case, log the fact of failed attempts

  Not the “bad” passwords!

  And monitor the log

  Talk to user to see if there is something wrong

- Note: lockout enables easy DoS attack
- Automatic lockout may make it hard to change your password if you have many devices

12

Fighting Guessing Attacks, contd.

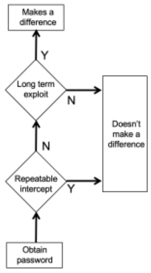
10

- What should "N" be?
- Advantages of a small N (<5)
  - Catch guessing attacks faster
    - Very slightly faster, if the password is hard to guess (maybe 0.001% faster)
- Disadvantages of a small N
  - Discourage the use of different passwords for different systems
  - Encourage the use of easy to type passwords
  - Encourage writing passwords down
- My recommendation: N = 10

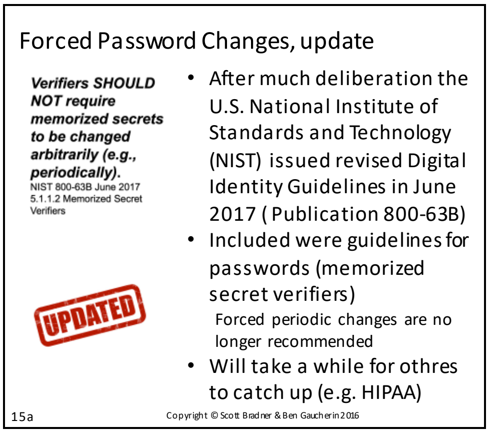
Forced Password Changes

- Common requirement - forced change of password every *N* days
  - Legally required by HIPAA
  - Required by PCI security standards
  - Required by most auditors
- But does it make things safer?
  - Mostly, no
  - But if the law says you have to do it, it is safer (by definition) to do it

Forced Password Changes, contd.



- Do a flow chart:
  - Forced password change only useful if…
    - Attacker obtaining a password without cooperation and without monitoring (e.g., keystroke logger)
      - Otherwise attacker will just get the new password
    - AND, an exploit takes a long time
      - e.g., if I can create a business & send it a check for $100 M: I'll just do that and run
        - Likelihood of required password change happening between me getting a password and using it is very small

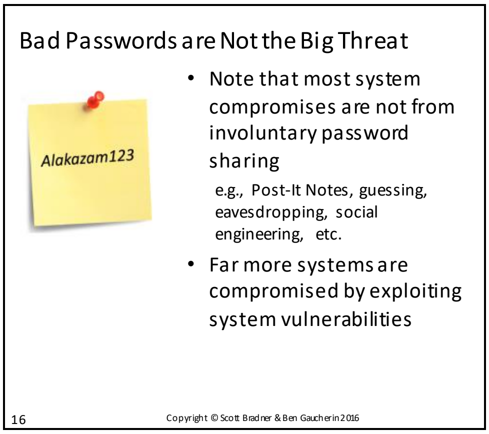


Forced Password Changes, update

Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).
NIST 800-63B June 2017
5.1.1.2 Memorized Secret Verifiers

UPDATED

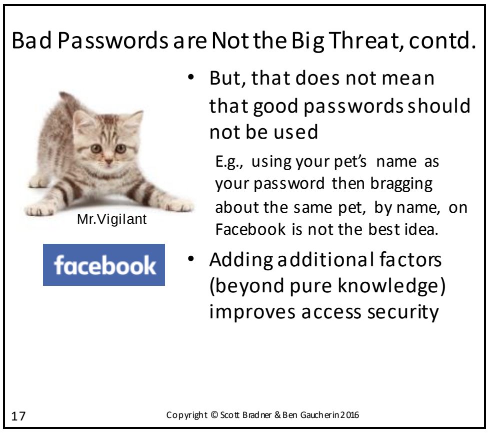
- After much deliberation the U.S. National Institute of Standards and Technology (NIST) issued revised Digital Identity Guidelines in June 2017 (Publication 800-63B)
- Included were guidelines for passwords (memorized secret verifiers)
  - Forced periodic changes are no longer recommended
- Will take a while for othres to catch up (e.g. HIPAA)



Bad Passwords are Not the Big Threat

Alakazam123

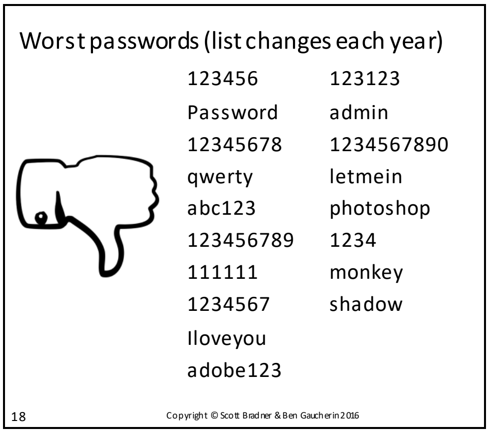
- Note that most system compromises are not from involuntary password sharing
  - e.g., Post-It Notes, guessing, eavesdropping, social engineering, etc.
- Far more systems are compromised by exploiting system vulnerabilities



Bad Passwords are Not the Big Threat, contd.

Mr.Vigilant

- But, that does not mean that good passwords should not be used
  - E.g., using your pet's name as your password then bragging about the same pet, by name, on Facebook is not the best idea.
- Adding additional factors (beyond pure knowledge) improves access security



Worst passwords (list changes each year)

123456	123123
Password	admin
12345678	1234567890
qwerty	letmein
abc123	photoshop
123456789	1234
111111	monkey
1234567	shadow
Iloveyou	
adobe123	

18

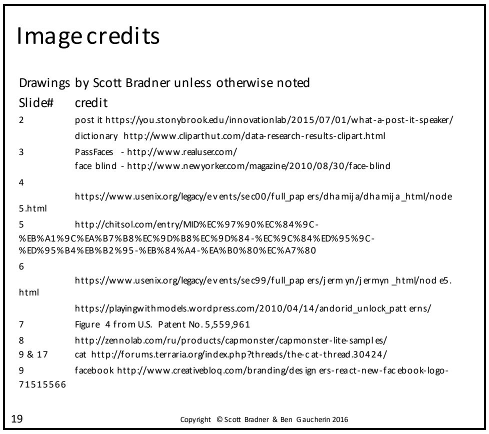


Image credits

Drawings by Scott Bradner unless otherwise noted

Slide#	credit
2	post it https://you.stonybrook.edu/innovationlab/2015/07/01/what-a-post-it-speaker/ dictionary http://www.cliparthut.com/data-research-results-clipart.html
3	PassFaces - http://www.realuser.com/ face blind - http://www.newyorker.com/magazine/2010/08/30/face-blind
4	https://www.usenix.org/legacy/events/sec00/full_papers/dhamija/dhamija_html/node5.html
5	http://chitsol.com/entry/MID%EC%97%90%EC%84%9C-%EB%A1%9C%EA%B7%B8%EC%9D%B8%EC%9D%84-%EC%9C%84%ED%95%9C-%ED%95%B4%EB%B2%95-%EB%84%A4-%EA%B0%80%EC%A7%80
6	https://www.usenix.org/legacy/events/sec99/full_papers/jermyn/jermyn_html/node5.html https://playingwithmodels.wordpress.com/2010/04/14/andorid_unlock_patterns/
7	Figure 4 from U.S. Patent No. 5,559,961
8	http://zennolab.com/ru/products/capmonster/capmonster-lite-samples/
9 & 17	cat http://forums.terraria.org/index.php?threads/the-cat-thread.30424/
9	facebook http://www.creativebloq.com/branding/designers-react-new-facebook-logo-71515566

19

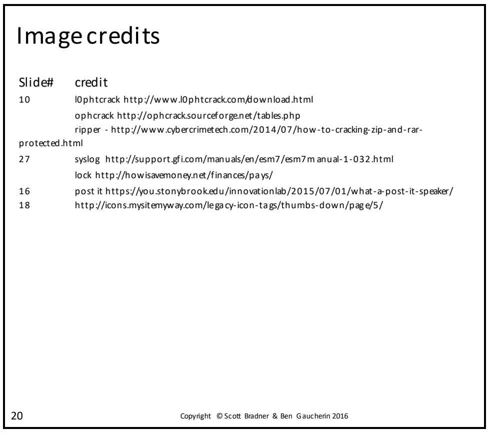


Image credits

Slide#	credit
10	l0phtcrack http://www.l0phtcrack.com/download.html ophcrack http://ophcrack.sourceforge.net/tables.php ripper - http://www.cybercrimetech.com/2014/07/how-to-cracking-zip-and-rar-protected.html
27	syslog http://support.gfi.com/manuals/en/esm7/esm7manual-1-032.html lock http://howisavemoney.net/finances/pays/
16	post it https://you.stonybrook.edu/innovationlab/2015/07/01/what-a-post-it-speaker/
18	http://icons.mysitemyway.com/legacy-icon-tags/thumbs-down/page/5/

20

Identity and authentication

Authentication - has

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Something a Person *Has*

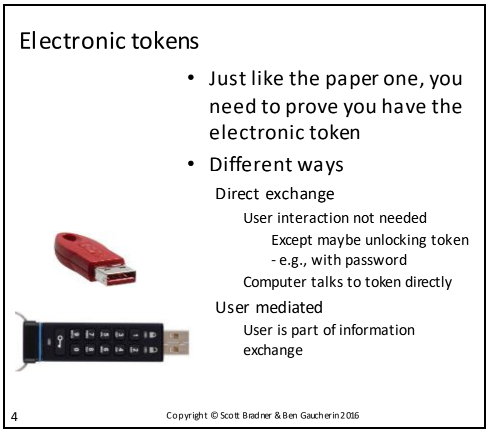
- Paper documents
  - Present document to authenticate yourself
- Electronic tokens
  - Key fobs, USB dongles, pocket cards, PDAs or laptops with special software
  - Must prove to the system that you have the token
    - Require presentation of token or an interaction with token

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Paper documents

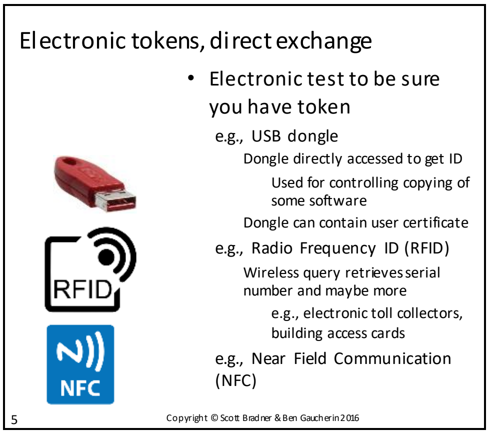
- Many examples
  - Drivers license, passport, health card, national ID card, work ID
- Two classes
  - Possession-based
    - You just need to have it - e.g., baseball game ticket
  - With physical identification information on document
    - e.g., signature, photo, thumb print, biometric
- Adding RFIDs to some paper documents
  - e.g., passports

3 Copyright © Scott Bradner & Ben Gaucherin 2016



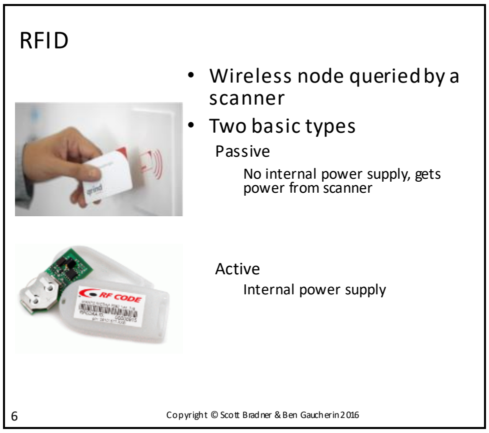
Electronic tokens

- Just like the paper one, you need to prove you have the electronic token
- Different ways
  - Direct exchange
    - User interaction not needed
      - Except maybe unlocking token - e.g., with password
    - Computer talks to token directly
  - User mediated
    - User is part of information exchange



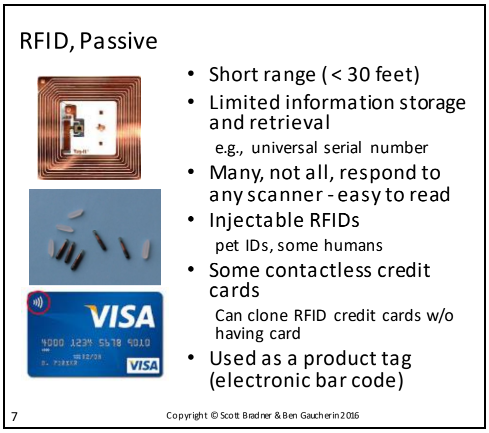
Electronic tokens, direct exchange

- Electronic test to be sure you have token
  - e.g., USB dongle
    - Dongle directly accessed to get ID
      - Used for controlling copying of some software
    - Dongle can contain user certificate
  - e.g., Radio Frequency ID (RFID)
    - Wireless query retrieves serial number and maybe more
      - e.g., electronic toll collectors, building access cards
  - e.g., Near Field Communication (NFC)



RFID

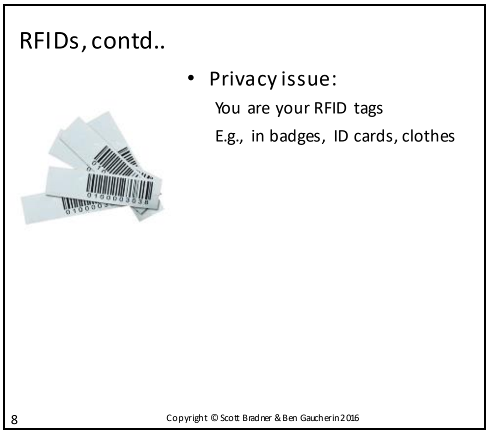
- Wireless node queried by a scanner
- Two basic types
  - Passive
    - No internal power supply, gets power from scanner
  - Active
    - Internal power supply



RFID, Passive

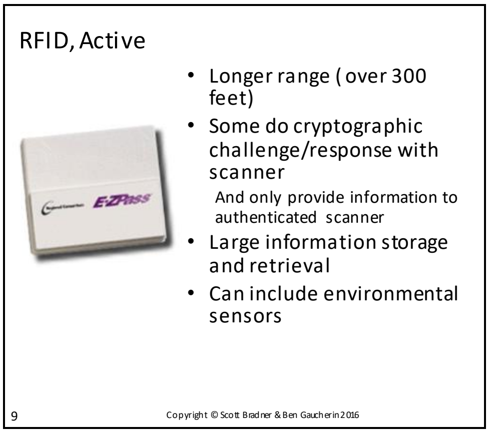
- Short range (< 30 feet)
- Limited information storage and retrieval
  - e.g., universal serial number
- Many, not all, respond to any scanner - easy to read
- Injectable RFIDs
  - pet IDs, some humans
- Some contactless credit cards
  - Can clone RFID credit cards w/o having card
- Used as a product tag (electronic bar code)

VISA
4000 1234 5678 9010
VISA



RFIDs, contd..

- Privacy issue:
  - You are your RFID tags
  - E.g., in badges, ID cards, clothes



RFID, Active

- Longer range (over 300 feet)
- Some do cryptographic challenge/response with scanner
  - And only provide information to authenticated scanner
- Large information storage and retrieval
- Can include environmental sensors

Electronic tokens, user mediated

- Login information

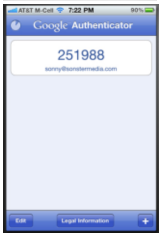
  user has token that produces information needed for login

- Challenge-response

  User has token or software to accept challenge & a secret password and produce response

- "Token" can be a standalone device or software to run on a laptop or PDA

Electronic tokens, login information



- e.g., RSA SecureID

  Token provides new "random" number every minute

  User provides ID (e.g., username)

  Server uses ID to determine which token user has

  Looks up seed for pseudo-random number generator in token

  Determines what number should be on token display

  Prompts user for number being currently displayed

  User enters value

  Server checks response against calculated value

Secure ID, Issues

- RSA creates & keeps "seeds" for each token

  Seed defines pseudo-random number sequence

  Other vendors let customers create & keep seeds

- RSA was hacked (disclosed March 2011)

  Hack was based on spear phishing

  Attached file "2011 Recruitment Plan" included a Flash 0-day bug

  Seeds stolen

Secure ID, Issues, contd.

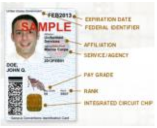
- Lockheed Martin hacked (disclosed May 2011)
  - Lockheed Martin said hack involved Secure IDs

LOCKHEED MARTIN

Login Information, contd.

- Some tokens require the user to enter a PIN into the token to generate the login information
- To ensure a stolen token is not a security threat
  - Cannot generate proper information without the right PIN

Electronic tokens, challenge-response



SAMPLE
BLOOD TYPE
DoD BENEFITS NUMBER
SHORT IMAGE
DATE OF BIRTH
GENEVA CONVENTION CATEGORY
DoD IDENTIFICATION NUMBER (ALSO USED AS THE GENEVA CONVENTIONS NUMBER)

- e.g., CRYPTOCard RB-1
  - User logs into system
  - System sends user a N-digit challenge
  - User enters challenge into token
  - Token generates response
  - User enters response into system
- e.g., US DoD Common Access Card
  - Plugs into local reader
  - Includes PKI certificate
  - Required for remote access

Electronic tokens, challenge-response, contd.

- Two-factor authentication using your phone

Basic sequence:

- Connect to authentication service
- Identify yourself (e.g. logname & password)
- Authentication service communicates with phone
- e.g.,
  - Sends code via SMS or data connection – you enter code
  - Calls phone & speaks code – you enter code
  - Queries app on phone, displays OK? – you press "yes"

Image credits

Drawings by Scott Bradner unless noted

Slide#	credit
2	http://www.bhphotovideo.com/c/buy/USB-License-Keys/ci/12454/N/4294550039
3	ticket http://chicagotix.com/SB-XL-on.shtml
	passport http://www.kimeshan.com/2013/07/16/when-things-go-wrong-abroad
	license http://community.beliefnet.com/dondiegodelavega/blog/2012/06/17/famous_drivers_licenses.
4	red key http://www.carrollcommunications.com/license/license.html
	black key http://www.apricorn.com/aegis-secure-key.html
5	red key http://www.carrollcommunications.com/license/license.html
	rfid - https://icons8.com/web-app/2350/rfid-signal
	nfc https://icons8.com/web-app/2305/nfc-sign
6	passive rfid http://www.secureattend.com/
	active rfid http://www.realtimeid.com/technology.htm
7	coil http://www.rfidvirus.org/
	injectable http://www.aliexpress.com/item/Small-pets-implanted-electronic-chip-imports-of-pet-animal-injectable-RFID-tags-grain-size/1984597668.html
	card http://www.cyberguy.com/appearances/how-to-beat-a-digital-pickpocket/
8	http://nexqo.manufacturer.globalsources.com/si/6008839817759/pdtl/RFID-sticker/1064302308/Jeans-hang-tag.htm

Image credits

Slide#	credit
9	http://www.nh.gov/dot/org/operations/turnpikes/ezpass/
11	https://en.wikipedia.org/wiki/RSA_SecurID
	http://iphone.appstorm.net/reviews/secure-your-life-with-google-authenticator/
13	http://logos.wikia.com/wiki/File:Lockheed-martin-logo.png
14	http://www.emc.com/collateral/data-sheet/h13821-ds-rsa-securid-hardware-tokens.pdf
15	crypto card http://portal.cryptocard.com/documentation/TechDocs/RB-1QUICKReference-2.pdf
	CAC card views http://www.cac.mil/common-access-card/
16	desk phone http://lestarihutanes.blogspot.com/2013/03/2500-basic-desk-phone.html
	flip phone https://en.wikipedia.org/wiki/Flip_%28form%29
	iPhone http://thesweetsetup.com/rene-ritchies-sweet-iphone-setup/

Identity and authentication

Authentication - is

CSCI E 45b: The Cyber World – part B

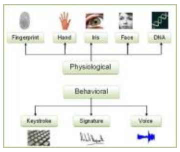
Some characteristic of you

RELEVÉ DU SIGNALEMENT ANTHROPOMÉTRIQUE

1. Taille. — 2. Envergure. — 3. Buste. — 4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. — 7. Pied gauche. — 8. Médius gauche. — 9. Coudée gauche.

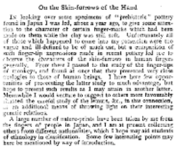
- Use characteristics of a person to identify or verify the identity of that person
  - Compare against a stored template to verify
  - Compare against a database of templates to identify
    - Security risk if central storage
- Varying degrees of reliability
- Not just physical characteristics
  - Also handwriting, gait, etc.
- Known as biometrics

Biometrics



- Physical factors
  - Finger, palm, foot, retina, iris & face prints, DNA, hand geometry, speech, vascular patterns
- Other factors
  - Typing, handwriting, gait
- Different factors have different levels of assurance
- Most useful for authentication not for identification

Biometrics, Fingerprints



On the Skin-furrows of the Hand

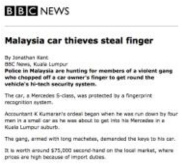
In looking over some specimens of "prehistoric" pottery found in Japan I was led, about a year ago, to give some attention to the character of certain finger-marks which had been made on them while the clay was still soft. Unfortunately all of those which happened to come into my possession were too vague and ill-defined to be of much use, but a comparison of such finger-tip impressions made in recent pottery led me to observe the characters of the skin-furrows in human fingers generally. From these I passed to the study of the finger-tips of monkeys, and found at once that they presented very close analogies to those of human beings. I have here few opportunities of prosecuting the latter study to much advantage, but hope to present such results as I may attain in another letter. Meanwhile I would venture to suggest to others more favourably situated the careful study of the lemurs, &c., in this connection, as an additional means of throwing light on their interesting genetic relations.

A large number of nature-prints have been taken by me from the fingers of people in Japan, and I am at present collecting others from different nationalities, which I hope may aid students of ethnology in classification. Some few interesting points may here be mentioned by way of introduction.

- First biometric identification
  - Understood as unique at least as early as 1860
  - Formal use for identification started in 1880s
    - Dr. Henry Faulds published article in Nature (1880)
      - Also performed 1st identification from a latent fingerprint
    - Mark Twain - murderer identified by thumb print in *"Life on the Mississippi"* (1883)
  - National collection of fingerprints in US - 1905

4

Biometrics, Fingerprints, contd.



BBC NEWS

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

The gang, armed with long machetes, demanded the keys to his car.

It is worth around $75,000 second-hand on the local market, where prices are high because of import duties.

- Fingerprint scanners can be spoofed
  - e.g., by gummy fingers, MythBusters & photo
- Fingerprint readers can be a threat to finger owner
  - e.g., car thieves cut off car owner's finger to try to steal a car - (*New Straits Times* - 31 October 2005)

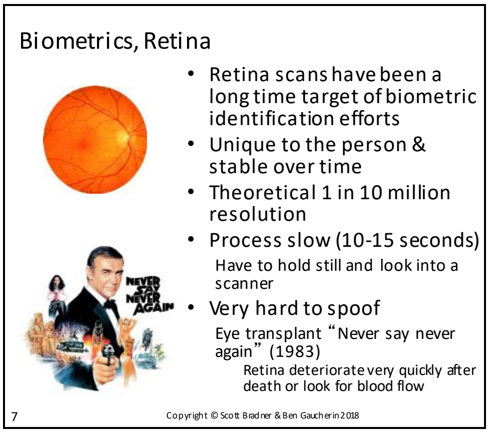
5

Biometrics, Fingerprints, contd.

- Readers are getting better
  - e.g., looking for the right temperature and blood flow in "finger" being scanned
  - But are still susceptible to peel-off fingerprints
- Fingerprint readers built into many devices
  - Beware devices that store full fingerprints
- Fingerprint stored in secure enclave on Apple iPhone & Mac – cannot be extracted

UPDATED

6

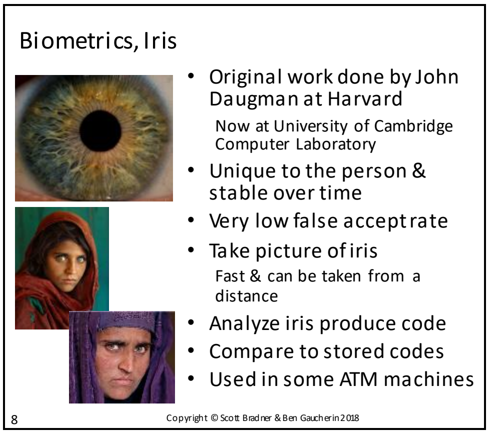


Biometrics, Retina

- Retina scans have been a long time target of biometric identification efforts
- Unique to the person & stable over time
- Theoretical 1 in 10 million resolution
- Process slow (10-15 seconds)
  - Have to hold still and look into a scanner
- Very hard to spoof
  - Eye transplant "Never say never again" (1983)
    - Retina deteriorate very quickly after death or look for blood flow

7

Copyright © Scott Bradner & Ben Gaucherin 2018

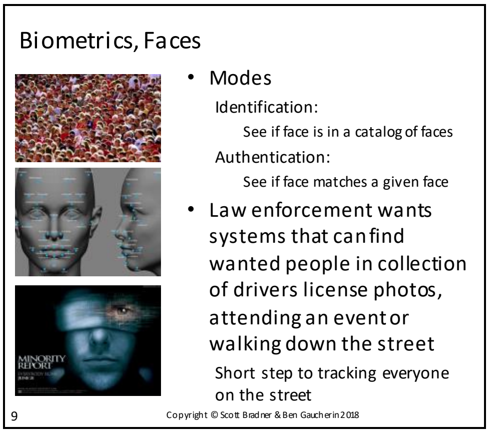


Biometrics, Iris

- Original work done by John Daugman at Harvard
  - Now at University of Cambridge Computer Laboratory
- Unique to the person & stable over time
- Very low false accept rate
- Take picture of iris
  - Fast & can be taken from a distance
- Analyze iris produce code
- Compare to stored codes
- Used in some ATM machines

8

Copyright © Scott Bradner & Ben Gaucherin 2018



Biometrics, Faces

- Modes
  - Identification:
    - See if face is in a catalog of faces
  - Authentication:
    - See if face matches a given face
- Law enforcement wants systems that can find wanted people in collection of drivers license photos, attending an event or walking down the street
  - Short step to tracking everyone on the street

9

Copyright © Scott Bradner & Ben Gaucherin 2018

Biometrics, Faces, Authentication

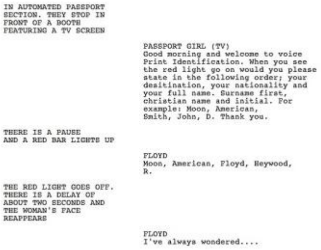
- Apple Face ID
  - First of many systems that will use a face to unlock a smartphone
- Face ID unlocks an iPhone that has been trained to a particular face when the user actually looks at the iPhone
- The system uses 30K infrared dots projected on the face to generate a map
  - Map compared with map stored in the secure enclave in the iPhone (same as Touch ID)

UPDATED

Biometrics, Hand Geometry

- Check shape of hand against database
- In use for access control since the 1980s
- Generally used with other IDs
  - e.g., ID cards

Biometrics, Speech



IN AUTOMATED PASSPORT SECTION. THEY STOP IN FRONT OF A BOOTH FEATURING A TV SCREEN

PASSPORT GIRL (TV)
Good morning and welcome to voice Print Identification. When you see the red light go on would you please state in the following order; your desitination, your nationality and your full name. Surname first, christian name and initial. For example: Moon, American, Smith, John, D. Thank you.

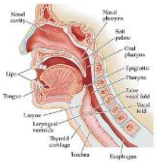
THERE IS A PAUSE AND A RED BAR LIGHTS UP

FLOYD
Moon, American, Floyd, Heywood, R.

THE RED LIGHT GOES OFF. THERE IS A DELAY OF ABOUT TWO SECONDS AND THE WOMAN'S FACE REAPPEARS

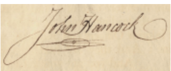
FLOYD
I've always wondered....

Biometrics, Speech, contd.



- a.k.a., "Voice Biometrics"
- User speaks specific words
  - Some systems require multiple readings
- System compares digitized voice against stored template for person
- Generally used along with other factors
- Not (yet) reliably used for authentication

Biometrics, Handwriting



- Signatures among earliest identification methods
  - e.g., sign a check
- Unique to an individual
- More than just signature capture
  - Used for package delivery & credit card use
- e.g., sign name on a tablet
  - Sequence, pressure, acceleration, timing of strokes measured
    - Not just resulting image
- Can track changes over time

Biometrics, Keystroke Recognition

- Multiple factors measured on keyboard
- e.g.,
  - The length of time each key is held down
  - The length of time between keystrokes
  - Typing speed
  - Tendencies to switch between a numeric keypad and keyboard numbers
  - The keystroke sequences involved in capitalization
- Problems if person injured, tired, cold, etc.

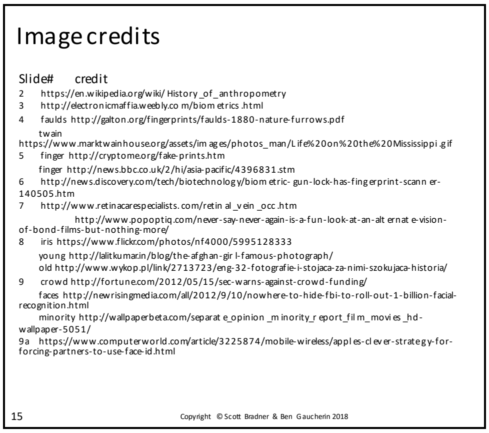


Image credits

Slide#	credit
2	https://en.wikipedia.org/wiki/History_of_anthropometry
3	http://electronicmaffia.weebly.com/biometrics.html
4	faulds http://galton.org/fingerprints/faulds-1880-nature-furrows.pdf
	twain https://www.marktwainhouse.org/assets/images/photos_man/Life%20on%20the%20Mississippi.gif
5	finger http://cryptome.org/fake-prints.htm
	finger http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
6	http://news.discovery.com/tech/biotechnology/biometric- gun-lock-has-fingerprint-scanner-140505.htm
7	http://www.retinacarespecialists.com/retinal_vein_occ.htm
	http://www.popoptiq.com/never-say-never-again-is-a-fun-look-at-an-alternate-vision-of-bond-films-but-nothing-more/
8	iris https://www.flickr.com/photos/nf4000/5995128333
	young http://lalitkumar.in/blog/the-afghan-girl-famous-photograph/
	old http://www.wykop.pl/link/2713723/eng-32-fotografie-i-stojaca-za-nimi-szokujaca-historia/
9	crowd http://fortune.com/2012/05/15/sec-warns-against-crowd-funding/
	faces http://newrisingmedia.com/all/2012/9/10/nowhere-to-hide-fbi-to-roll-out-1-billion-facial-recognition.html
	minority http://wallpaperbeta.com/separate_opinion_minority_report_film_movies_hd-wallpaper-5051/
9a	https://www.computerworld.com/article/3225874/mobile-wireless/apples-clever-strategy-for-forcing-partners-to-use-face-id.html

15 Copyright © Scott Bradner & Ben Gaucherin 2018

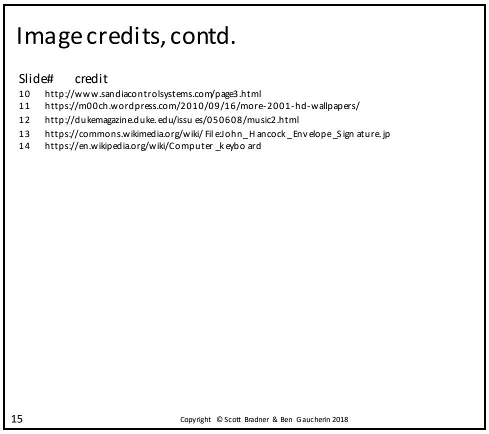


Image credits, contd.

Slide#	credit
10	http://www.sandiacontrolsystems.com/page3.html
11	https://m00ch.wordpress.com/2010/09/16/more-2001-hd-wallpapers/
12	http://dukemagazine.duke.edu/issues/050608/music2.html
13	https://commons.wikimedia.org/wiki/File:John_Hancock_Envelope_Signature.jp
14	https://en.wikipedia.org/wiki/Computer_keyboard

15 Copyright © Scott Bradner & Ben Gaucherin 2018

Identity and authentication

Authentication – multi factor

CSCI E 45b: The Cyber World – part B

Multiple factors help

- Multiple factors significantly increases the reliability of authentication
  - e.g., ATM
  - Must have physical ATM card and knowledge of correct PIN
- But does not help against some common attacks
  - See Bruce Schneier - *The Failure of Two-Factor Authentication*

Multi-factor, details

- Requires two or more factors
  - User knows, user has, user is
- Multiple checks of one factor is not multi-factor
  - Two or more passwords
  - Two or more biometric measurements
- Smart cards, by themselves, are not multi-factor
  - They are just a more reliable way to identify a card

Multi-factor, the most common approach

- Something "you know" and something "you have" (i.e., a password, and a mobile phone)
  - Can be an issue if the user is traveling outside of their calling zone
- Uses temporary code

Mobile phone based multi-factor

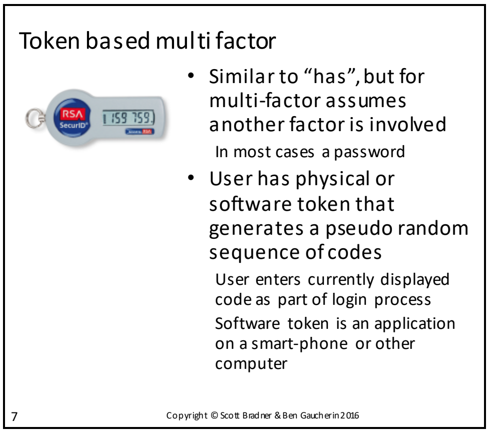
UPDATED

Note: insecure method because SMS is very easy to hack

- Call with a code
  - System calls the phone and speaks a code
  - User enters code during login
- Call for a code
  - System shows code on web page and calls user on phone
  - User enters code into phone using push buttons
- SMS a code
  - System sends an SMS message to the phone with a code
  - User enters code during login

Mobile phone based multi-factor, contd.

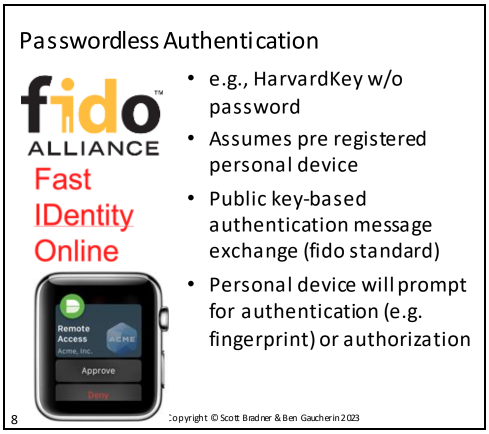
- Communicate with application on mobile phone
  - System interacts with app on phone, e.g. user shown "yes" and "no" buttons to press
- Other factors and phone features can also be used (e.g., GPS, camera, fingerprint reader, etc.)


RSA
SecurID
159 759

Token based multi factor

- Similar to “has”, but for multi-factor assumes another factor is involved
  - In most cases a password
- User has physical or software token that generates a pseudo random sequence of codes
  - User enters currently displayed code as part of login process
  - Software token is an application on a smart-phone or other computer

7


fido
ALLIANCE
Remote
Access
Acme, Inc.
ACME
Approve
Deny

Passwordless Authentication

Fast
IDentity
Online

- e.g., HarvardKey w/o password
- Assumes pre registered personal device
- Public key-based authentication message exchange (fido standard)
- Personal device will prompt for authentication (e.g. fingerprint) or authorization

8

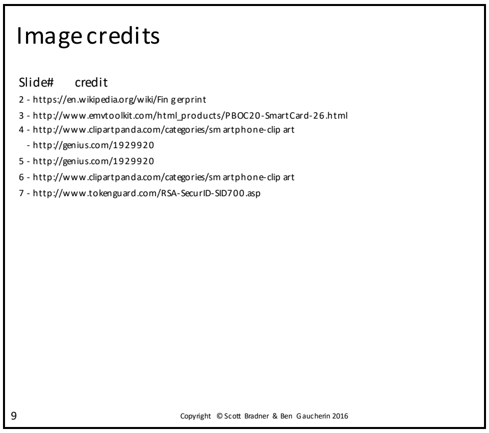


Image credits

Slide# credit

2 - https://en.wikipedia.org/wiki/Fingerprint

3 - http://www.emvtoolkit.com/html_products/PBOC20-SmartCard-26.html

4 - http://www.clipartpanda.com/categories/smartphone-clip art

- http://genius.com/1929920

5 - http://genius.com/1929920

6 - http://www.clipartpanda.com/categories/smartphone-clip art

7 - http://www.tokenguard.com/RSA-SecurID-SID700.asp

9

Identity and authentication

Issues

CSCI E 45b: The Cyber World – part B

Mutual Authentication

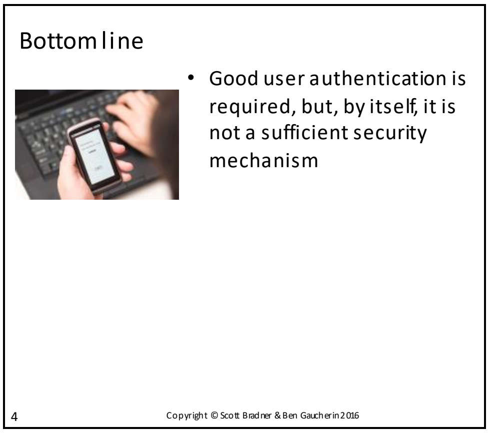
You know who I am
But who are you?

Unicode:
semicolon (;)
Greek question mark (;)

- You may have a great password but how do you know that you are logging into the right site?
- Server certificates help but not all systems or applications use them
  - And they are not error free
    - e.g., UNICODE characters in domain name

Only Part of the Problem

- Note that the best passwords or multi-factor authentication will not protect a system from a user that:
  - Opens email attachments from strangers
  - Responds to phishing attacks
  - Surfs porn sites that download malware
  - Downloads the world to an unencrypted laptop then loses it
  - Uses same password for porn site as for company site
  - …



Bottom line

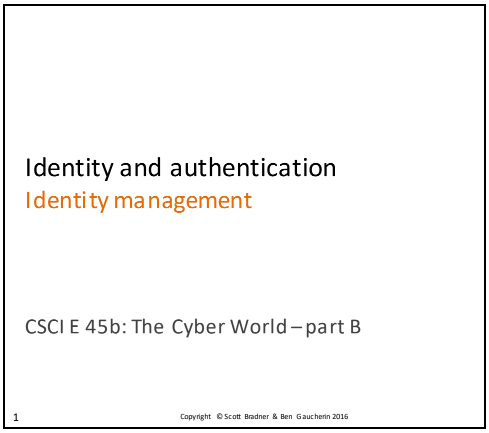
- Good user authentication is required, but, by itself, it is not a sufficient security mechanism

4 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
4	https://www.certivox.com/blog/bid/320343/2-step-verification-vs-2-factor-authentication

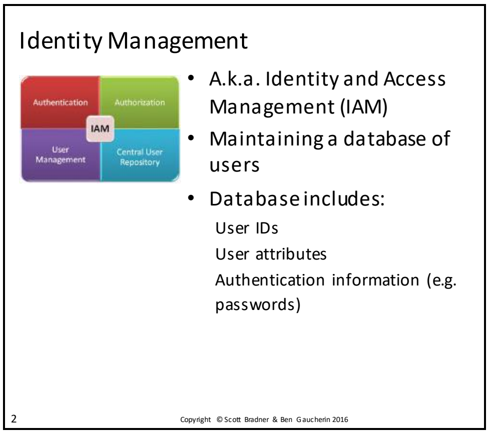
5 Copyright © Scott Bradner & Ben Gaucherin 2016



Identity and authentication

Identity management

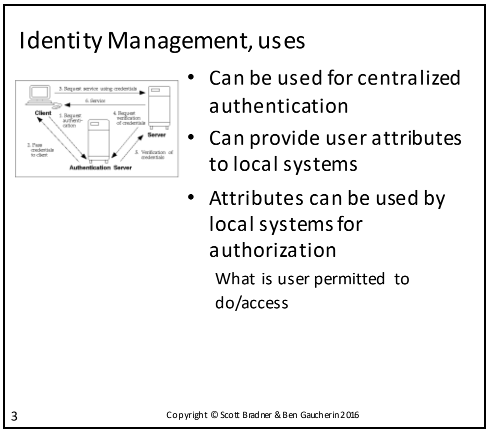
CSCI E 45b: The Cyber World – part B



Identity Management

Authentication
Authorization
IAM
User Management
Central User Repository

- A.k.a. Identity and Access Management (IAM)
- Maintaining a database of users
- Database includes:
  - User IDs
  - User attributes
  - Authentication information (e.g. passwords)



Identity Management, uses

3. Request service using credentials
6. Service
Client
1. Request authentication
4. Request verification of credentials
Server
2. Pass credentials to client
5. Verification of credentials
Authentication Server

- Can be used for centralized authentication
- Can provide user attributes to local systems
- Attributes can be used by local systems for authorization
  - What is user permitted to do/access

User attributes

First Name: John
Last Name: Smith
Employee ID: 1234567
Email: js@example.com
Office: 14-623
Title: Managing Director
Role: employee

Grouper™

- Personal information
  - Name, email address, office location
- Organizational IDs
- Organizational Role(s)
- Group(s)
  - Used for authorization
  - Some populated from other attributes, some manually

Identity management, issues

ONBOARD
MANAGE
SUPPORT
DEACTIVATE

- Feeds from systems of record
- ID lifetime
  - Creation of new IDs
  - Tracking status and job changes
    - Including termination
  - ID reuse?
- Assigning multiple IDs to same person
- Multiple people assigned the same ID
  - E.g., because of similar names

Image credits

Slide#	credit
2	http://www.quoinx.com/identity_access_management.html
3	https://docs.oracle.com/cd/A57673_01/DOC/net/doc/NWANO233/ch1.htm
4	grouper - http://www.internet2.edu/products-services/trust-identity-middleware/grouper/
5	http://hitachi-id.com/largedocs/presentation-kc-iam-cloud-2011/12.html

Identity and authentication

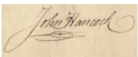
Conclusion

CSCI E 45b: The Cyber World – part B

Identities & authentication

- An identity is a identifier for a person
  - Whether you know who the person is or not
- Authentication is binding an identity to a unique person
- The process of authentication requires an identifier and a way to verify that the person is the right person for the identifier

Four types of authentication verifiers



- Knowledge-based
  - What a person knows
    - E.g. passwords
- Possession-based
  - What a person has
    - E.g., RSA token
- Biometric-based
  - What a person is
    - e,.g., fingerprint
- Action-based
  - What a person can do
    - E.g. signature

Multi-factor authentication

- Require two or more types of authentication for authentication

  E.g. password and token

Identity management

Authentication
Authorization
IAM
User Management
Central User Repository

- Need to maintain an accurate inventory of people for authentication to be useful

  E.g. a database of active employees and their passwords and token identifiers

Image credits

Slide#	credit
2	SS card - https://www.flickr.com/photos/metropolismusic/2667617635
	ticket - http://www.ebay.com/itm/321653479266
3	horse: U.S. Patent No. 5,559,961
	red key http://www.carrollcommunications.com/license/license.html
	iris https://www.flickr.com/photos/nf4000/5995128333
	signature: https://commons.wikimedia.org/wiki/File:John_Hancock_Envelope_Signature
4	black key http://www.apricorn.com/aegis-secure-key.html
5	http://www.quoinx.com/identity_access_management.html