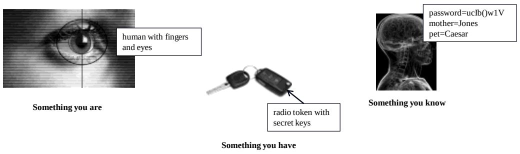
Identification and Authentication

Authentication is the binding of an identity to a subject

Authentication

- The determination of **identity**, usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys)
  - something the person knows (like a password)
  - something the person is (like a human with a fingerprint)
  - where the person is (secure building, parking lot)



Klein sample of 15,000 passwords

8%	Dictionary words
4%	Common names
3%	User/account name
2%	Phrases, patterns
1%	Male names
1%	Female names
1%	Uncommon names
1%	Machine names
1%	Place names
1%	King James Bible

Categories of Easily Guessed PWs

- Based on an account
  - account name followed by number
  - account name surrounded by delimiters
- Based on a user’s name
  - Initials repeated 0 or more times
  - All letters upper (or lower) case
  - Name reversed
  - First initial followed by last name reversed
- Dictionary word
- Dictionary with words spelled backwards
- Dictionary word with all or some letters capitalized

- Reversed dictionary word with all or some letters capitalized
- Dictionary word with arbitrary letter turned into a control character
- Pattern from the keyboard
- Contains only digits
- Looks like a license plate number
- Acronyms (e.g., UCSB, DOD, ACM, IEEE)
- Concatenation of dictionary words
- Dictionary words with all vowels deleted

Gramp and Morris
Unix Operating System Security (1984)

- If login is abc

  Try abc, cba, abcabc
- Comments field
- Finger
- 20 most common female names each followed by a single digit yielded at least one password on every system tried

Gramp and Morris Suggestions

- Make it difficult for an outsider to get a copy of the password file
- Remove encrypted passwords from the password file and put in a parallel file unreadable to the public and UUCP
- Remove comment field
- Modify password program to check for and prevent weak passwords
- Educate users about good and bad passwords or assign passwords

Proactive Password Checking

- Analyze proposed password for "goodness"
  - Always invoked
  - Can detect, reject bad passwords for an appropriate definition of "bad"
  - Discriminate on per-user, per-site basis
  - Needs to do pattern matching on words
  - Needs to execute subprograms and use results
    - Spell checker, for example
  - Easy to set up and integrate into password selection system

Storage

- Store as cleartext
  - If password file compromised, *all* passwords revealed
- Encipher file
  - Need to have decipherment, encipherment keys in memory
  - Reduces to previous problem
- Store one-way hash of password
  - If file read, attacker must still guess passwords or invert the hash

One-way Cipher

An irreversible function **f** from plaintext to ciphertext. It is computationally infeasible to determine a plaintext message M from the ciphertext **C = f(M)**

Unix crypt()

MD5

Unix Crypt( ) Algorithm

- DES with first eight characters of password as the key
- Iterated 25 times on constant 0
- E-table modified to depend on 12-bit salt
  - This is so that DES chip cannot be used for fast encryption
- Final 64 bits are unpacked into a string of 11 printable characters

Salt

12-bit random number that is appended to the password supplied by a user

Thus, 4096 encrypted versions of each password

Increases the work of checking a given string against a list of encrypted passwords

Example

kemm:3hWG9n3yrXmw6:2010:3033:Richard Kemmerer:/home/kemm:/bin/tcsh

3hWG9n3yrXmw6

nBRIcGosLI76w

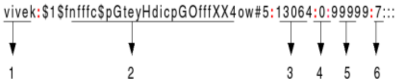
glaTgrS8galyw

Shadow Password File

- Shadow file contains encrypted passwords
  /etc/shadow
- Shadow file is protected from being read
- Password field in /etc/passwd is blank or contains a special symbol or random value

kemm:x:2010:3033:Richard Kemmerer:/home/kemm:/bin/tcsh

Shadow Password File Entries



```
vivek:$1$fnfffc$pGteyHdicpGOfffXX4ow#5:13064:0:99999:7:::
```

#1: Username

#2: Password: $algorithm$salt$hashed_pass

#3: Day password last changed
(in days past epoch)

#4-6: Min/Max/Warn
Password change settings.

Crypt(3) Hash Function Codes

On GNU/Linux:

- Default (no code): DES
- "$1$" stands for MD5
- "$2$" is Blowfish
- "$5$" is SHA-256
- "$6$" is SHA-512

SHA512-crypt ($6$)

Based on SHA-512 but designed for use with crypt(3)

- 86 character encoded checksum result
- 1000-999999999 rounds (default 5000)
- 16 character salt

- Design rationale and reference C implementation: http://www.akkadia.org/drepper/SHA-crypt.txt

SHA512 Example

wormhole:$6$nQqdclku7raBh8ag$K63.Jo.weK8Qa9y5KXDqCo/6zZFQjAnh3AUYX/LI9reugdE.vFH

LDAP Server

- Lightweight Directory Access Protocol
- Internet protocol that email and other programs use to look up information from a server
- Used at UCSB for "single sign-on" to many services

Computer Generated Passwords

3sed77yo

TT6sw45

xc_56RR

Passphrase

- User friendly passwords generated by combining symbols where each symbol is a pronounceable word
- Based on phoneme
  - cv, vc, cvc, vcv
    (e.g., **helgoret** or **juttelon**)
- Number of pronounceable passwords of length n is considerably less than number of random passwords of length n

Tunable Passwords

System gives the user part of a password

User constructs new password according to specified rules

Bishop Advice for Strong Passwords

Password should contain at least one of each of the following

- digit
- letter
- punctuation symbol
- control character

Writing Down Passwords

- If you absolutely need to write down a password you should use some transformation scheme such that what is written down is transformed to the actual password
- Bishop gives the following scheme:
  - Capitalize the third letter
  - Add 2 to the end
    (e.g., **TuzLeb7** is transformed to **TuZLeb72**)

Password Aging

- The idea is that in the time it takes to guess a password it will no longer be valid
- Force users to change passwords after some time has expired
  - How do you force users not to re-use passwords?
    - Record previous passwords
    - Block changes for a period of time
  - Give users time to think of good passwords
    - Don't force them to change before they can log in
    - Warn them of expiration days in advance

Dictionary Attacks

- Trial-and-error from a list of potential passwords
  - *Off-line*: know *one-way function* and *enciphered passwords*, and repeatedly try different guesses until the list is done or passwords guessed
    - Examples: *crack*, *john-the-ripper*
  - *On-line*: have access to system functions and try guesses until some *guess* succeeds
    - Examples: trying to log in by guessing a password

Type 2 Dictionary Attacks

- The attacker uses the actual login, su, etc. function to try the guess
- Defense is to slow down the attack through
  - backoff
  - disconnection
  - disable
  - jailing

Password Sniffers

- Monitor all information sent over a local area network
- Record the first 20, 50, 128 characters sent over each network connection

One-Time Passwords

- Password that can be used exactly *once*
  - After use, it is immediately invalidated
- Challenge-response mechanism
  - Challenge is number of authentications; response is password for that particular number
- Problems
  - Synchronization of user, system
  - Generation of good random passwords
  - Password distribution problem

Code Book

- List of passwords that are used one time and then never used again
- User looks up next password in the code book
- Can have mathematical algorithm to generate list, then list can be virtual

S/Key

- One-time password scheme based on idea of Lamport
- *h* one-way hash function (MD5 or SHA-1, for example)
- User chooses initial seed *k*
- System calculates:

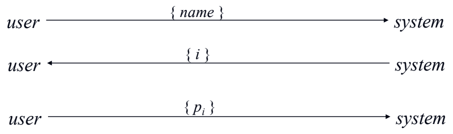
$$h(k) = k_1,\ h(k_1) = k_2,\ \ldots,\ h(k_{n-1}) = k_n$$

- Passwords are reverse order:

$$p_1 = k_n,\ p_2 = k_{n-1},\ \ldots,\ p_{n-1} = k_2,\ p_n = k_1$$

S/Key Protocol

System stores maximum number of authentications n, number of next authentication i, last correctly supplied password p_{i-1}



System computes $h(p_i) = h(k_{n-i+1}) = k_{n-i+2} = p_{i-1}$. If match with what is stored, system replaces p_{i-1} with p_i and increments i.

Token Cards

- Card has some calculation based on the time and a secret function or serial number
  - Time sensitive
  - Challenge-response
  - May require a user pin

SecurID Card

Displays a number that changes every 30-90 seconds

SecureNet Key

- When user logs into a remote machine it displays a number as a challenge
- User enters his/her pin and challenge into the card
- Card returns a response, which the user sends to the remote machine
- Card can be programmed to self-destruct when the wrong pin is entered a certain number of times

SecureNet Key Loader

Biometric and Behavioral Systems

- Depend on unique physiological and behavioral characteristics that can be examined and quantified
- Obtains data from you, converts it to digital representation, and compares it to stored sample
- Should be used in a two-factor authentication system
  - e.g., with passwords

Requirements for Biometric and Behavioral Identification

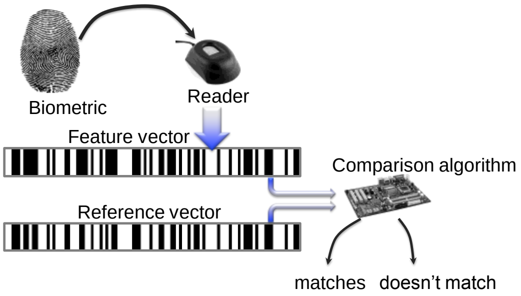
- **Universality.** Almost every person should have this characteristic
- **Distinctiveness.** Each person should have noticeable differences in the characteristic
- **Permanence.** The characteristic should not change significantly over time
- **Collectability.** The characteristic should have the ability to be effectively determined and quantified

Biometrics

- **Biometric** refers to any measure used to uniquely identify a person based on biological or physiological characteristics
- Generally, biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before granting access

Image from http://commons.wikimedia.org/wiki/File:Fingerprint_scanner_in_Tel_Aviv.jpg used with permission under the Creative Commons Attribution 3.0 Unported license

Biometric Identification



Biometric

Reader

Feature vector

Comparison algorithm

Reference vector

matches

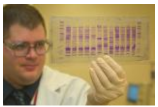
doesn’t match

Candidates for Biometric IDs

- Fingerprints
- Retinal/iris scans
- DNA
- Face recognition

Public domain image from http://commons.wikimedia.org/wiki/File:Fingerprint_Arch.jpg

Public domain image from http://commons.wikimedia.org/wiki/File:Retinal_scan_securimetrics.jpg



Public domain image from http://commons.wikimedia.org/wiki/File:CBP_chemist_reads_a_DNA_profile.jpg

Consider how each of these scores in terms of universality, distinctiveness, permanence, and collectability…

Candidates for Behavioral IDs

Test patterns of physiology or behavior

- “Blue-ink” signature
- Voice recognition
- Gait recognition
- Keystroke pattern

Again, consider how each of these scores in terms of universality, distinctiveness, permanence, and collectability…

Ranking in Order of

Effectiveness

- retina pattern
- fingerprint
- handprint
- voice pattern
- keystroke pattern
- signature

Personal Acceptance

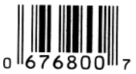
- keystroke pattern
- signature
- voice pattern
- handprint
- fingerprint
- retina pattern

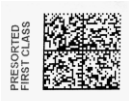
Two-factor Authentication Technology

- Barcodes
- Magnetic stripe cards
- Smart cards
- SIM cards
- RFIDs

Barcodes

- Developed in the 20th century to improve efficiency in grocery checkout.
- First-generation barcodes represent data as a series of **variable-width, vertical lines** of ink, which is essentially a one-dimensional encoding scheme
- Some more recent barcodes are rendered as **two-dimensional patterns** using dots, squares, or other symbols that can be read by specialized optical scanners, which translate a specific type of barcode into its encoded information





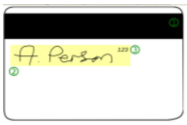
Authentication via Barcodes

- Since 2005, the airline industry has been incorporating two-dimensional barcodes into boarding passes, which are created at flight check-in and scanned before boarding
- In most cases, the barcode is encoded with an internal unique identifier that allows airport security to look up the corresponding passenger's record with that airline
- Staff then verifies that the boarding pass was in fact purchased in that person's name (using the airline's database), and that the person can provide photo identification
- In most other applications, however, barcodes provide convenience but not security. Since barcodes are simply images, they are extremely easy to duplicate

Public domain image from http://commons.wikimedia.org/wiki/File:Bpass.jpg

Magnetic Stripe Cards

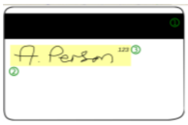
- Plastic card with a magnetic stripe containing personalized information about the card holder
- The first track of a magnetic stripe card contains the cardholder's full name in addition to an account number, format information, and other data
- The second track may contain the account number, expiration date, information about the issuing bank, data specifying the exact format of the track, and other discretionary data



Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Magnetic Stripe Card Security

- One vulnerability of the magnetic stripe medium is that it is easy to read and reproduce
- Magnetic stripe readers can be purchased at relatively low cost, allowing attackers to read information off cards
- When coupled with a magnetic stripe writer, which is only a little more expensive, an attacker can easily clone existing cards
- So, many uses require card holders to enter a PIN to use their cards (e.g., ATM and debit cards in the U.S.)



Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Smart Cards

- **Smart cards** incorporate an integrated circuit, optionally with an on-board microprocessor with reading and writing capabilities, allowing the data on the card to be both accessed and altered
- Smart card technology can provide secure authentication mechanisms that protect the information of the owner and are extremely difficult to duplicate

Public domain image from http://en.wikipedia.org/wiki/File:Carte_vitale_anonyme.jpg

Smart Card Authentication

- They are commonly employed by large companies and organizations as a means of strong authentication using cryptography
- Smart cards may also be used as a sort of "electronic wallet," containing funds that can be used for a variety of services, including parking fees, public transport, and other small retail transactions

SIM Cards

- Many mobile phones use a special smart card called a **subscriber identity module card (SIM card)**
- A SIM card is issued by a network provider. It maintains personal and contact information for a user and allows the user to authenticate to the cellular network of the provider

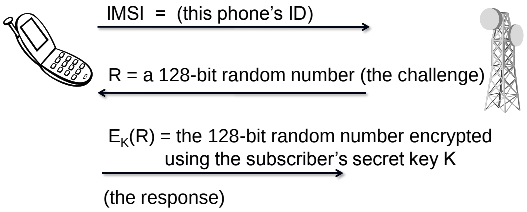
SIM Card Security

- SIM cards contain several pieces of information that are used to identify the owner and authenticate to the appropriate cell network
- Each SIM card corresponds to a record in the database of subscribers maintained by the network provider
- A SIM card features an **integrated circuit card ID (ICCID)** which is a unique 18-digit number used for hardware identification
- Next, a SIM card contains a unique **international mobile subscriber identity (IMSI),** which identifies the owner's country, network, and personal identity
- SIM cards also contain a 128-bit **secret key.** This key is used for authenticating a phone to a mobile network
- As an additional security mechanism, many SIM cards require a PIN before allowing any access to information on the card

GSM Challenge-Response Protocol

1. When a cellphone wishes to join a cellular network it connects to a local **base station** owned by the network provider and transmits its IMSI
2. If the IMSI matches a subscriber's record in the network provider's database, the base station transmits a 128-bit random number to the cellphone
3. This random number is then encoded by the cellphone with the subscriber's secret key stored in the SIM card using a proprietary encryption algorithm known as **A3,** resulting in a ciphertext that is sent back to the base station
4. The base station then performs the same computation, using its stored value for the subscriber's secret key. If the two ciphertexts match, the cellphone is authenticated to the network and is allowed to make and receive calls

GSM Challenge-Response Protocol



IMSI = (this phone's ID)

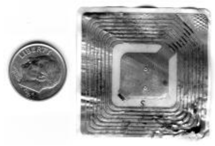
R = a 128-bit random number (the challenge)

$E_K(R)$ = the 128-bit random number encrypted using the subscriber's secret key K

(the response)

RFIDs

- **Radio frequency identification, or RFID,** is a rapidly emerging technology that relies on small transponders to transmit identification information via radio waves.
- RFID chips feature an integrated circuit for storing information, and a coiled antenna to transmit and receive a radio signal.



RFID Technology

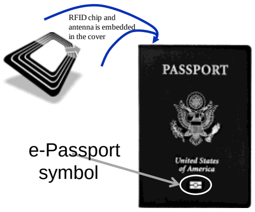
- RFID tags must be used in conjunction with a separate reader or writer.
- While some RFID tags require a battery, many are passive and do not.
- The effective range of RFID varies from a few centimeters to several meters, but in most cases, since data is transmitted via radio waves, it is not necessary for a tag to be in the line of sight of the reader.

RFID Technology

- This technology is being deployed in a wide variety of applications.
- Many vendors are incorporating RFID for consumer-product tracking.
- Car key fobs.
- Electronic toll transponders.

Passports

- Modern passports of several countries, including the United States, feature an embedded RFID chip that contains information about the owner, including a digital facial photograph that allows airport officials to compare the passport's owner to the person who is carrying the passport.


RFID chip and antenna is embedded in the cover
PASSPORT
United States of America
e-Passport symbol