Identification & Authentication

Part 3 of 3

Stallings: ***Chapter 3, 22***

Lidinsky: ***Supplementary Material***

Overview

Passwords

Strong secure passwords, S/Key

PPP schemes

PAP, CHAP, EAP

Third party authentication systems

Kerberos, TACACS+, RADIUS

Discussed this during last 2 lectures.

Mutual authentication

Digital certificates

Tokens

Biometric authentication

Multifactor authentication

Federated Identity Management

Some other schemes

This lecture

Mutual Authentication

Mutual Authentication
Need

Until recently many authentication schemes have focused on party 1 authenticating to a trusted party 2

When you bank on-line, you send authentication info (name, PIN) to the bank

You assume that the bank web site is legitimate

But suppose a web site hijacker is impersonating the bank and you are really communicating with this malicious web site

You just gave the hijacker your name and PIN

She can turn around and deplete your accounts

Mutual Authentication

Lately there has been an increasing requirement for the two parties to identify with each other

Mutual authentication is the process by which each party in an electronic communication verifies the identity of the other party

We'll discuss this more in the next sections of this lecture

Digital Certificates

Digital Certificates

Electronic means of verifying identity of an individual or organization

Digital signature

Piece of data that claims that a specific, named individual wrote or agreed to the contents of an electronic document to which the signature is attached

Digital Certificate

Sort of a certified digital signature

It is often treated as such by the courts

CAs

Certificate authority (CA)

Trusted, third-party entity that verifies the actual identity of an organization or individual before providing a digital certificate

Nonrepudiation

Practice of using a trusted, third-party entity to verify the authenticity of a party who sends a message

Reputable CAs have several levels of authentication that they issue based on the amount of data collected from applicants

CA Examples: VeriSign, Entrust, Digicert…

PKI

Public Key Infrastructure

PKI Overview

A Problem with cryptography and systems

We know that we can use public keys for sending private keys, message authentication (signing of message), and data integrity

But how do Bob & Alice reliably and automatically determine each other's public keys?

PKI Goals

Provide services for protocols using public keys

Trusted key management

Trusted certificate management

PKI Standards

There are a number of PKI standards

Two of the most widely used are

X.509

RFC 5280

PKCS (Public Key Cryptography Standard)

PKI Overview
What is a X.509 Certificate?

An X.509 certificate contains the following:

Version of X.509 standard	Ver. 3 had the number 2
ID of certificate	Unique serial number
ID & Algorithm of issuing CA	e.g., enTrust, SHA1
ID of subject entity	Name assigned by X.509
Public Key & Algorithm of subject	e.g., bff7ade8… & RSA(2048)
Period that key is valid	*Starting, ending time & date*
Signature (thumbprint) algorithm	e.g., sha1
Signature (thumbprint) of CA	Authentication of CA e.g., 68 ed 18 b3…

Other optional stuff

The certificate relates a public key to a subject entity such as a person, corporation, etc.

PKI Overview
What's A Certificate Authority?

A CA is a trusted authority

- *A CA achieves trust by*
  - Investigating subject entities
  - Issuing public key pairs
  - Binding public keys to subject entities
- *Issues certificates authenticated (signed) by CA*
- *Revokes certificates*
- *Provides on line signed certificate revocation lists*

PKI Overview
What's A PKI?

A ***PKI*** is comprised of

- *ORA (Organizational Registration Authority) [NIST]*
  - Relates *Certificate Holders* to *public keys*
  - Guarantees the relationships
- *CA (Certificate Authority)*
  - Issues guaranteed *certificates*
  - Revokes certificates
  - Provides Certificate Revocation Lists

PKI Overview

Certificate Holders are the "subject entities" that have been issued certificates

The certificate enables the Certificate Holder to “sign” digital documents with a "certified" signature

Clients are able to validate digital signatures

By using certificates obtained from a CA in a trusted manner

PKI Simple Example

Alice is a manufacturer who makes widgets

Alice goes to a ORA (Organizational Registration Authority)

The ORA investigates Alice to make sure she's OK

The ORA then give the information to the CA

Bob now wants to buy widgets from Alice on-line

Bob tells Alice that he wants to buy some widgets

Alice tells Bob that he must be certified by the CA

Bob also goes to the ORA and, after the ORA investigates Bob, it give Bob's info to the CA

Now Bob and Alice have a trust mechanism

PKI Simple Example

Next Bob goes to the CA and requests Alice's certificate

The CA returns Alice's certificate to Bob

It includes Alice's public key, the time during which the key is valid and the CA's signature

Bob verifies the CA's signature

Bob now has a certified copy of Alice's public key

Alice does the same to get a certified version of Bob's public key

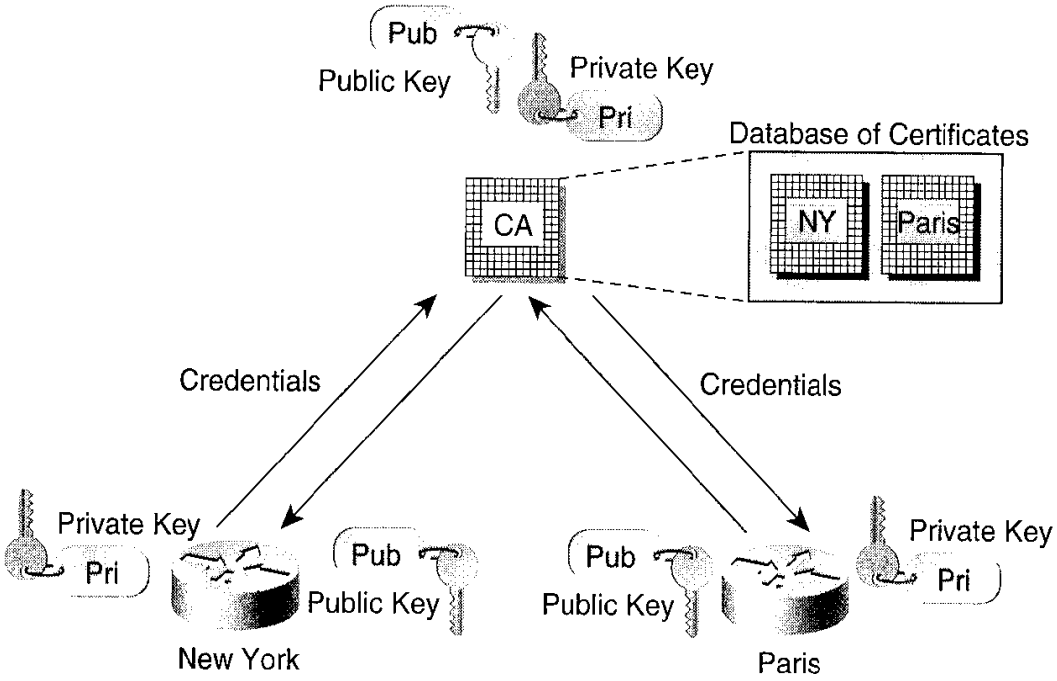
PKI Simple Example

Bob uses Alice's public key to place order and send money

Alice uses Bob's public key to assure the order

All transactions between Alice and Bob can be encrypted, signed, and have data integrity.

Router Example



The CA has certificates for both the NY and Paris routers in its database

Both routers know the CA's public key

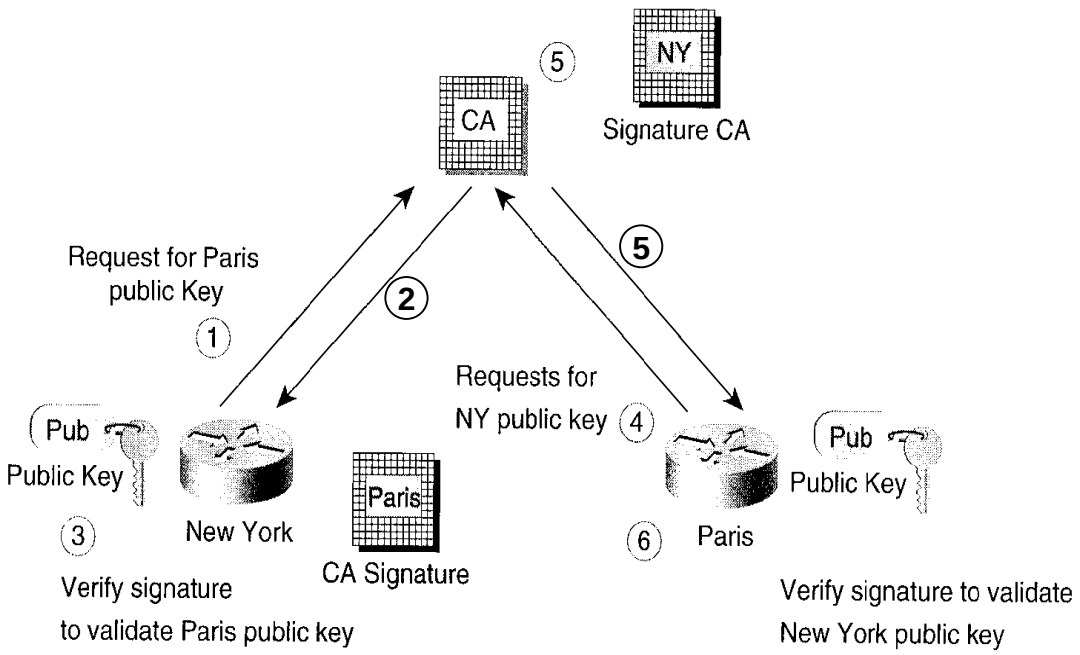
They both acquired it in some trusted way

Neither router knows the other router's public key

The NY router wants to send data to the Paris router

The Paris router wants it authenticated and encrypted

Router Example



1. NY router asks CA for Paris router's public key
2. CA sends NY router Paris router's public key in a certificate signed with CA's private key
3. NY verifies CA's certificate with CA's public key
4. Paris router asks CA for NY's public key
5. CA sends NY router's public key to Paris router in a certificate signed with CA's private key
6. Paris verifies CA's certificate with CA's public key

Both routers now have certified values for each other's public keys

7. Now the routers can use PGP or some similar scheme to send the data.

PKI Rationale

If there were no CA, then the NY router would need to keep a list of the public keys for all the routers with whom it might wish to securely communicate

With a CA, only one public key needs to be widely available

That of the CA

The public keys are certified as being valid

The public keys have a limited time

Minimizes replay attacks

OCSP Stapling

Helps deal with the certificate revocation problem

Won't discuss it here. Time!

Read about it at

http://en.wikipedia.org/wiki/OCSP_stapling

Tokens

Authentication Parameters

Access can be based upon what three things?

*Something that you **know***

*Something that you **have***

*Something that you **are***

Or combinations thereof

Security Tokens
Something You Have +

Authentication devices assigned to specific user

e.g., Your house key

e.g., Small, credit card-sized physical devices

Contains what is known as “base keys”

A token is an item that you have

Not something you know *or* are

But it also can be used in combination with something you know

Security Tokens
Something You Have +

Example

An ATM card that you have

Usually contains a "base key"

Plus the PIN that you must know

This is what is known as a ***two-factor*** authentication method

Security Tokens
Something You Have +

Advantage

Able to utilize **base keys** *that are much stronger than short, simple passwords a person can remember*

Disadvantage

If you loose the physical token or don't have it with you, you loose access to system

Types of Security Tokens

Types of tokens

- *Passive*
- *Active*
- *One-time*

Passive Tokens

Act as a storage device for the base key

Does not emit, or otherwise share base key

Example

- *ATM card*
  - Card holds a base key that is used to begin the transaction
  - A PIN is needed to use the token (ATM card)

Pros and Cons

- *Strong base keys*
- *Weak PINs*
- *Might be relatively easy to copy token information*

Active Tokens

Unlike passive tokens, active tokens not only store the base key but also:

They actively create another form of a base key such as an encrypted form of a base key

- *Encryption can be f(date or time or sequence)*
- *Not as vulnerable to attack by sniffing and replay*
- *But active tokens require some intelligence to generate the alternate form of the base key*
- *Can provide variable outputs in various circumstances*
- *Can store information*

Active Tokens

Usually a integrated circuit is built into the token

- *Intelligence and memory*

Active Token Example: “Smart cards”

- *Microprocessor built into the card*

Types of smart cards

- *Contact type*
  - Insert into the device being accessed
- *Contactless*
  - Doesn't insert, but manually transfer information from it
  - e.g., User looks at a display on the card and enters a number
- *Hybrid*

One-Time Tokens

Token generates a key that is used only once or for limited period of time; then is no longer valid

Uses shared keys and challenge-and-response systems, which do not require that the secret be transmitted or revealed

Strategies for generating one-time keys

Sequence-based tokens

Time-based tokens

These are basically active tokens combined with sequence value or time

Sequence-Based Tokens

Generally creates a strong one-time password

Password = f(secret long-term password & **sequence**)

To get a password

Contactless

Usually press a button on the token (card)

Copy the password that is displayed

Contact

Insert the token (card)

Password is generated automatically

Password is good once and for a limited amount of time

Time-Based Tokens

Almost identical to sequence-based tokens

Creates an equally strong one-time password

Password = f(secret long-term password & **time**)

Otherwise counter-based and time-based tokens are the same

One-Time Token Synchronization

- Counter or clock in the token and in server must be synchronized
  - *Requires accurate oscillators to drive the counters or the clocks*
  - *Economically possible today because of low cost highly accurate tiny quartz oscillators*
    - Same as those in your wrist watch
- But often there is some way to remotely resynchronize the counter or clock in the token with that in the server

Biometrics

Biometric Authentication
Something You Are

Something that you **are**

Uses measurements of physical or behavioral characteristics of an individual

e.g., fingerprint, handwritten signature, iris or retina pattern, voice recognition…

Generally considered the "best" of all authentication methods

Traditionally has been used in highly secure areas

Was very expensive

But cost has come down

There are privacy issues

How Biometric Authentication Works

Identity is verified

Physical feature (biometric) is scanned

Biometric information is analyzed and mapped into an electronic template

Template is stored

To gain access, biometric is scanned again

Computer analyzes biometric data and compares it to data in template

If data from scan matches data in template, person is allowed access

Unauthorized and Denied Access

False positive (incorrectly authorized access)

*Occurrence of an **un**authorized person being authenticated by a biometric authentication process*

Results in unauthorized access

False negative (incorrectly denied access)

*Occurrence of an authorized person **not** being authenticated by a biometric authentication process when they really are who they claim to be*

Results in legitimate access being denied

These are not an issue for what you ***know*** or ***have***. Why?

Different Kinds of Biometrics

Physical characteristics usually used

- *Fingerprints*
- *Hand geometry*
- *Retinal scanning*
- *Iris scanning*
- *Facial scanning*

Behavioral characteristics

- *Handwritten signatures*
- *Voice*

Fingerprint Biometrics

Many scanners are used today on:

- *Computers*
- *Smart phones*
- *Physical access scanners*
  - Usually mounted on a wall next to a door
- *External flash and rotating memory*
- *Web site*
- *Stand alone*

Fingerprint Biometrics

A fingerprint is a trace of the epidermal ridges of a finger

Today there are three accepted systems for characterizing fingerprints

Roscher, Vucetich, Henry

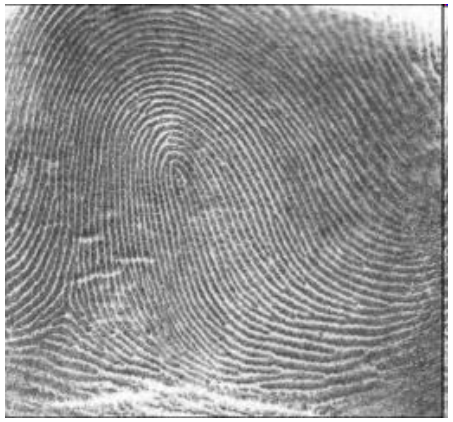
Henry scheme is the most commonly used

Consists of the relative locations of ***loops***, ***whorls*** and ***arches*** formed by the ridges

Often ***deltas*** are also used

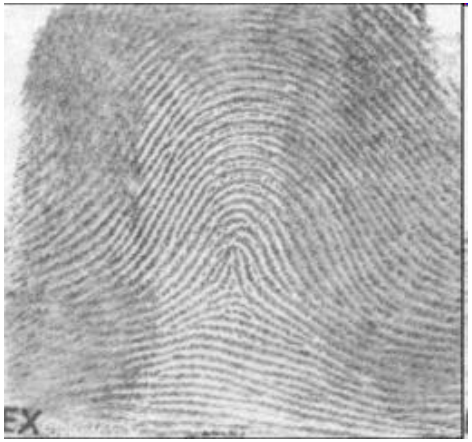
Fingerprint Examples

Simple Arch



Loop & Delta

Whorl



Tent Arch

Fingerprint Biometric Sensor Types

Optical

Images the finger

Finger and scanner must be clean

Ultrasonic

Captures the ridge patterns by the ultrasonic returns of the array of locations on the surface of the scanner

Cleanliness less of an issue

Fingerprint Biometric Sensor Types

Capacitance, passive

Captures the ridge patterns by the electrical values of the array of locations on the surface of the scanner

Finger and scanner must be clean

Capacitance, active

Similar to ultrasonic

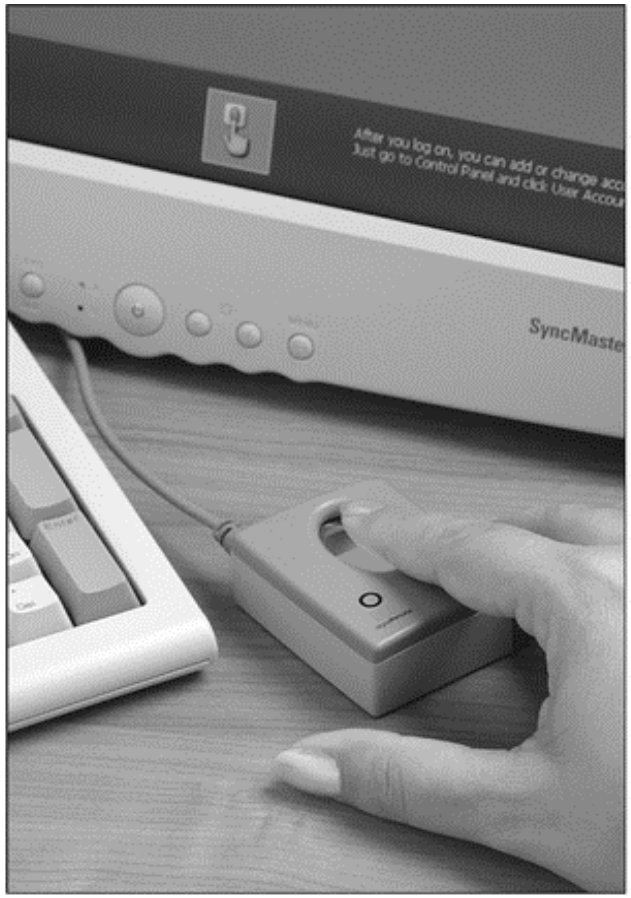
Thermal

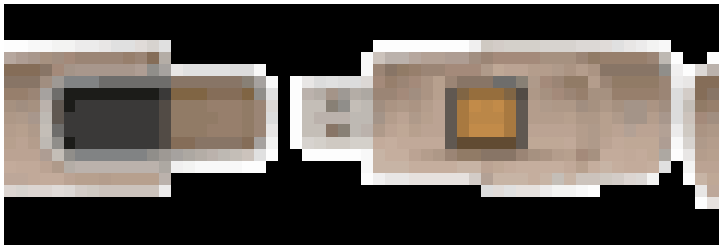
Reliability

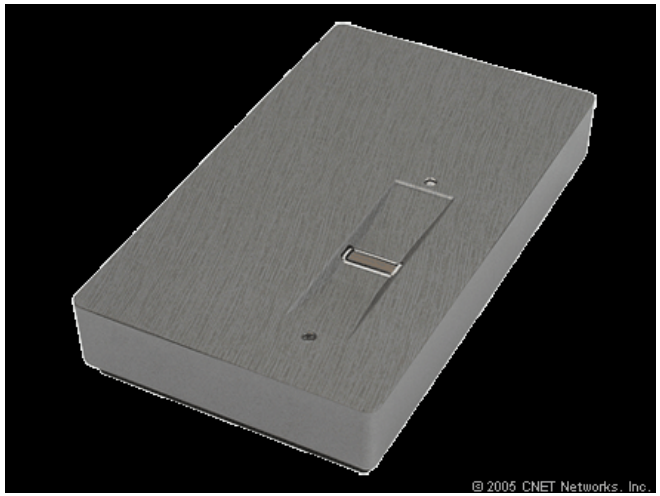
Only modest reliability

- *Image changes each time the scanner is touched*
- *Reliability could be better if several fingerprints were used*
- *There are now systems that use prints from multiple fingers*

Fingerprint Biometrics







Handprints

Identifies the person by the creases in their palms and upper fingers

Not considered as unique or accurate as other methods

Not used much

Handprint Example

Hand Geometry Authentication

Identifies the person by the shape of their hand or hands

Measure a user's hand along multiple dimensions

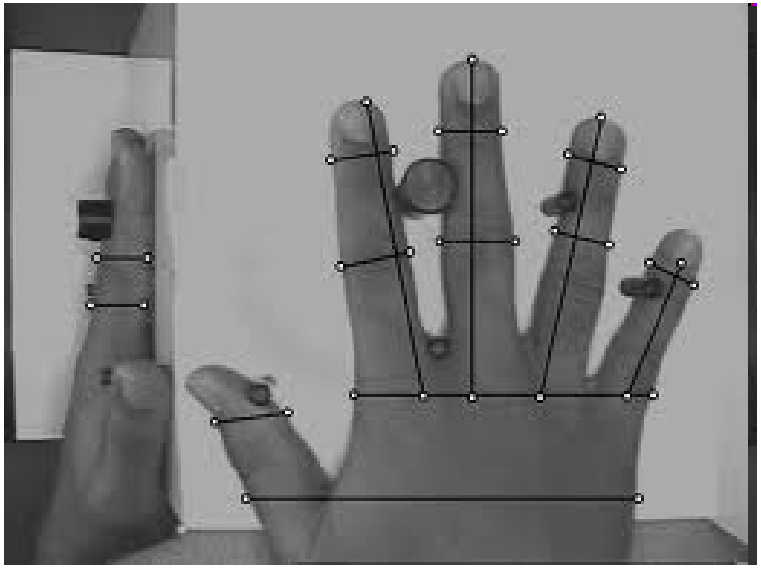
Not considered as unique as fingerprints or iris identification

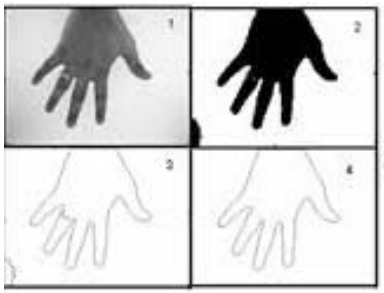
Used mostly for physical access or to control attendance

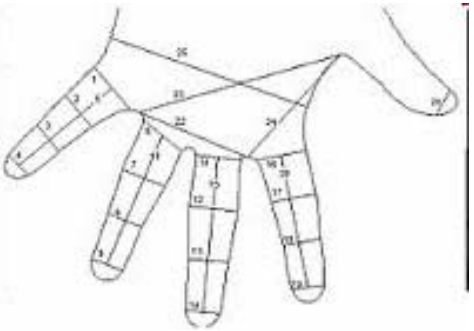
Scanners are large

So not used for computer access

Hand Geometry Authentication







Hand Geometry Authentication

Figure 2-7 Hand geometry scanner: HandkeyII by Recognition Systems Inc.

Retinal Scanning

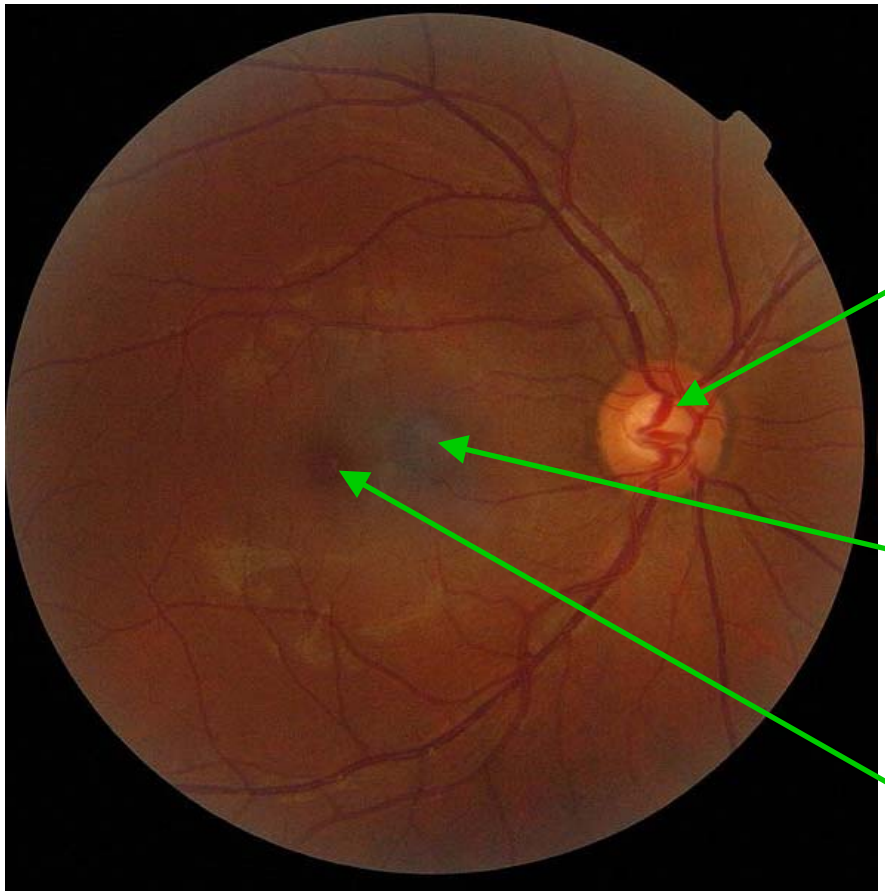
Takes an optical image of the retina

- *Measures the infrared pattern of the retina capillaries*

Retinal characteristics for biometric authentication

- *Relatively stable over the life of an individual*
- *Very accurate and distinctive*
- *Extremely hard to forge*
- *Expensive*
- *Low acceptance by users*
  - User must look directly into the scanner
  - Spreading germs and the laser scare

Retinal Scanning



Retinal Scanning

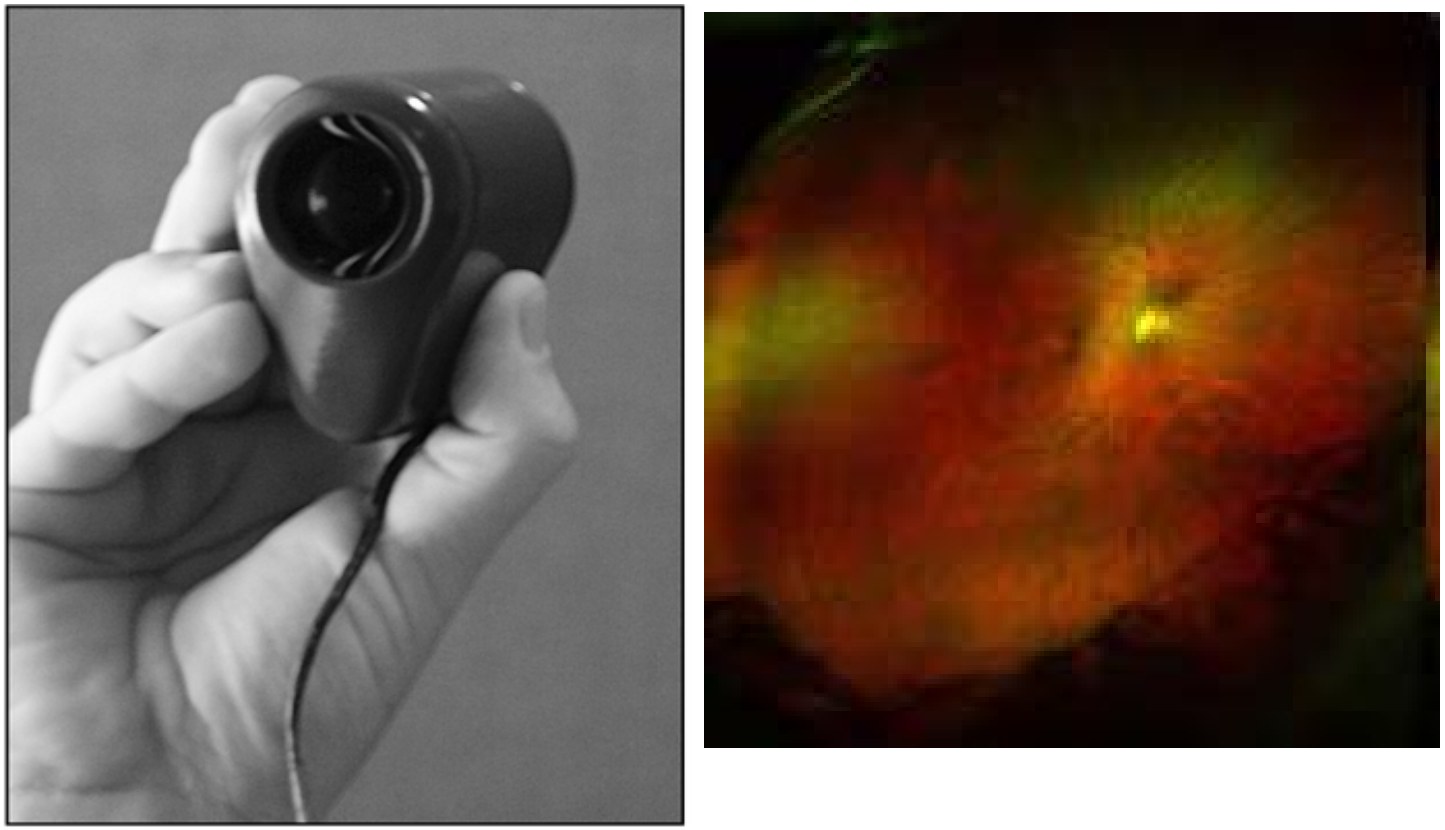


Figure 2-8 Retinal scanner by Eyedentify Inc.

Iris Recognition

Optically takes an optical or infrared image of the iris

An iris has a very detailed and unique structure

Relatively stable over the life of an individual

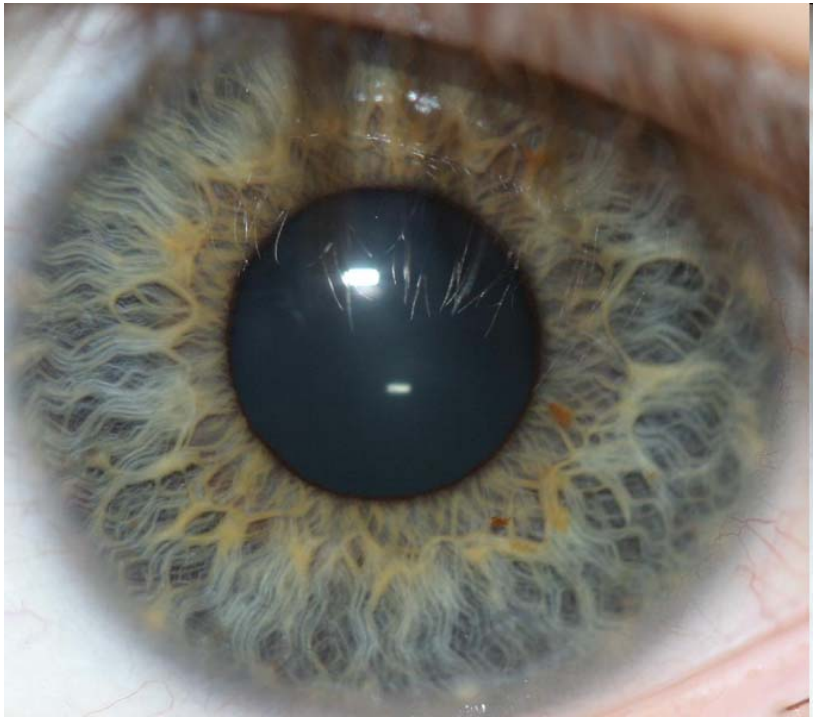
Costly

Public acceptance is not a problem as with retina scans

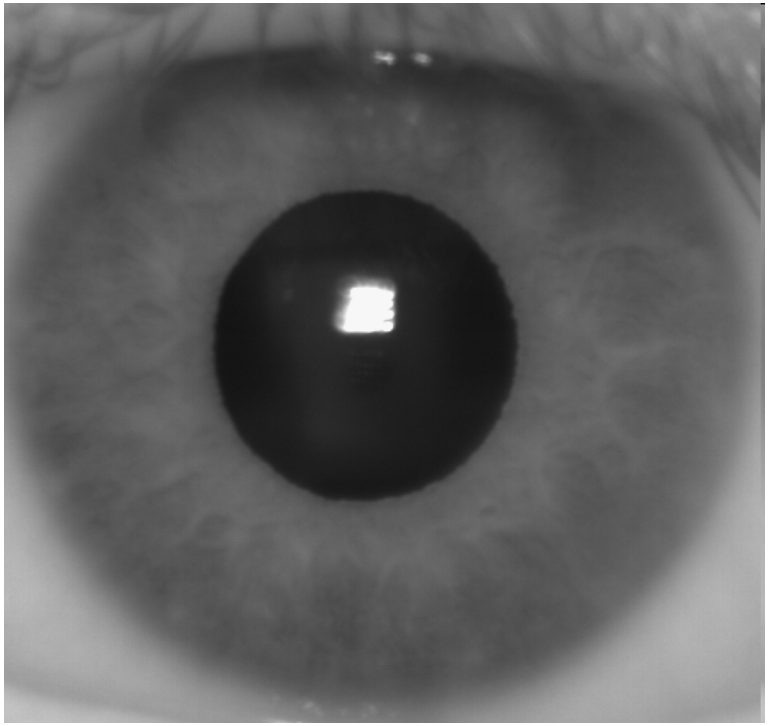
Can be performed at a distance of a few meters

Not the same a retinal scanning

Iris Images



Visible Light (VL) Image



Near Infrared Light (NIR) Image

NIR is not as good as VL, but still effective

Iris Scanning

Figure 2-9 Iris scanner by Panasonic Authenticam

Signature Verification

Has good accuracy

More easily forged

People are use to signing things

Not may systems available for automatic verification

The systems that you use when you buy something at stores such as Home Depot or Walgreen probably don't verify your signature

But to be sure I just mark an "X"

Signature Verification

Figure 2-10 Signature scanner by Interlink ePad VP9105

Voice Recognition

Other names

Speaker Recognition, Speaker Verification. Speaker Authentication, Voice Authentication

Recognizes who is speaking

Not the same as Speech Recognition that recognizes what is being said

Matches the words being spoken to a voice print

Training is required

Two types

Text dependent

Text independent

Voice Recognition
Text Dependent

Usually also requires speech recognition

e.g., User speaks a secret pass phrase or PIN

Can work with prompts for special knowledge

Can vary across several pieces of information

e.g., Your dog's name.

Next time, your birthday

Can also work across multiple users all with the same shared secret

Voice Recognition
Text Independent

Can be independent of words being used

Requires a prior voice print to be created based upon

- *Frequency*
- *Envelope*
- *Chirp decomposition and analysis*

Much math

- *Hidden Markov models*
- *Pattern matching*
- *Gaussian analysis*
- *Spatial to frequency matrix transforms*

Voice Recognition

Voice recognition is growing

Still not too accurate

Background noise, microphone quality, acoustics, allergies or a common cold, anxiety, being in a hurry, and anger can all alter the human voice enough to make voice recognition very difficult

Voice recognition systems tend to have the most difficult and time-consuming training process and require the most space for template storage.

Cell phone use has improved this technology for different uses

Face Recognition Schemes

Relative position and shape of facial features

- *Jaw, cheeks, eyes, nostrils…*
- *Image is not stored for comparison*
- *Distilled location and shape features are stored*
- *Some issues*
  - Lighting variation
  - Facial skewing (e.g., smiling, frowning…)

Face Recognition Schemes

Multiple Spectrum

- *Illuminate face with broad spectrum light*
- *Detect the face with detectors sensitive to different spectrums*
- *Then use relative position and shape*
- *Claims to be more accurate and reliable than*

3D recognition

- *Detects relative position and shape in 3 dimensions*
- *e.g., Jutting chin, deep eye sockets…*

There are other schemes as well

Face recognition

Available on PCs

Recently added to many smart phones

Not too secure, but probably will get better

Used at several Super Bowls

Being proposed for ATM machines

General Trends in Biometrics

Useful for authenticating large numbers of people over a short period of time

Smart cards can also be used effectively for this

Gaining remote access to controlled areas

Multifactor Authentication

Multifactor Authentication*

Identity of individual is verified using at least two of the three factors of authentication

- *Something that you know (eg, password, PIN)*
- *Something that you have (eg, smart card)*
- *Something that you are (eg, biometrics)*

What organizations might use multifactor authentication?

- *Been done for a long time using lower tech*

Federated Identity Management

FIM

Federated Identity Management*

Use of common identity management scheme

- *Across multiple enterprises & numerous applications*
- *Can support many thousands, even millions of users*
- *May result in cost savings due to added convenience and economies of scale*

Concepts

- *Identity management is centralized in a mutually trusted organization*
- *Defines a trusted identity for each principal (human, process…)*
- *Associates attributes with each identity*
- *Provides a means for verifying an identity*
- *Used to obtain access to Intranets of multiple participating enterprises*

Some FIM Elements

Authentication

Confirming user corresponds to the user name provided

Authorization

Granting access to services/resources given user authentication

Accounting

Process for logging access and authorization

Provisioning

Enrollment of users in the system

Workflow automation

Ability to move data around within the federation

delegated administration

Role-based access control to grant permissions

Some FIM Elements

Password synchronization

Facilitates single sign-on (SSO) or reduced sign-on (RSO) across participating organizations

Self-service password reset

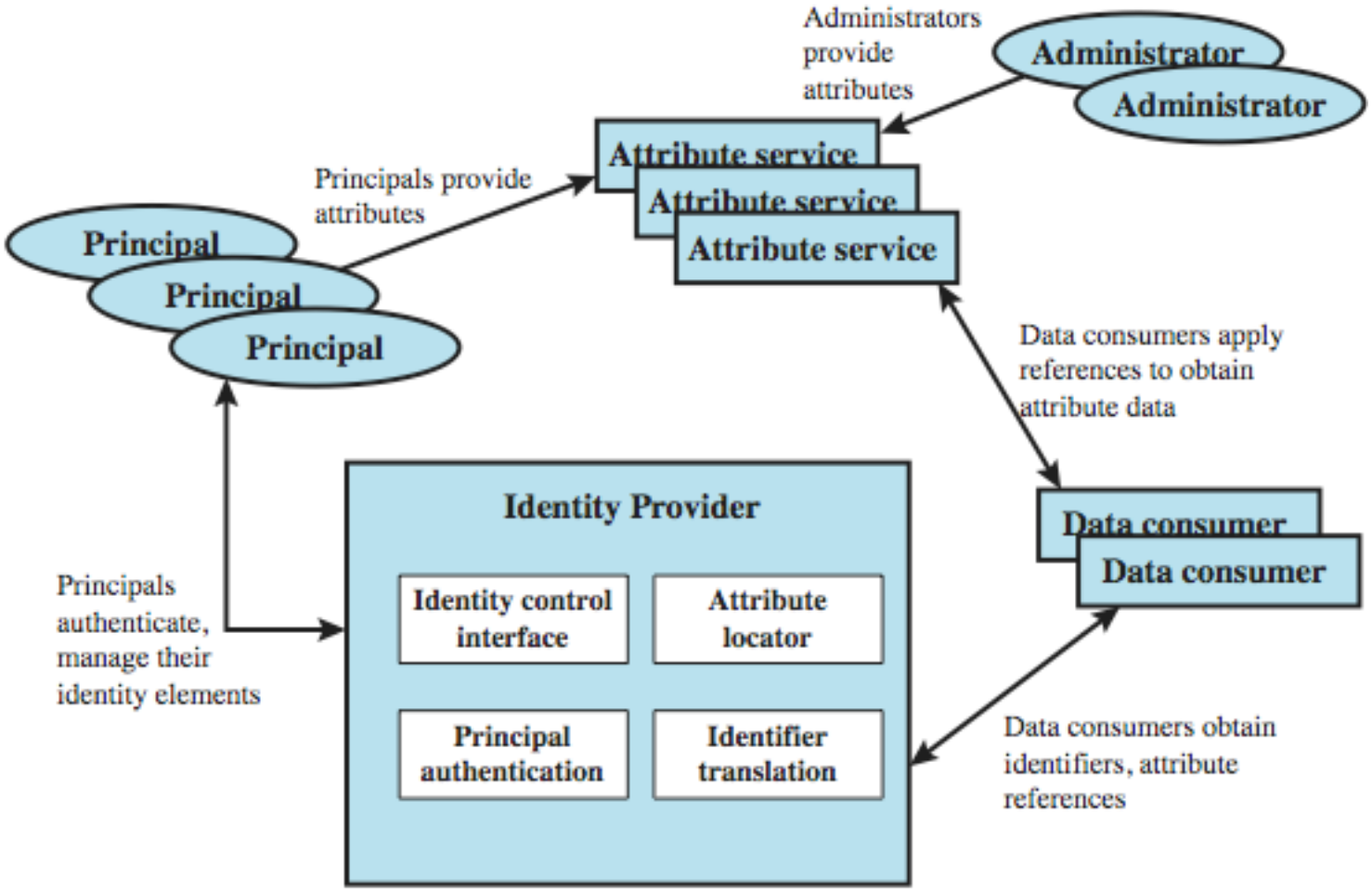
Users can change their own password and the change will propagate throughout the federation

Federation

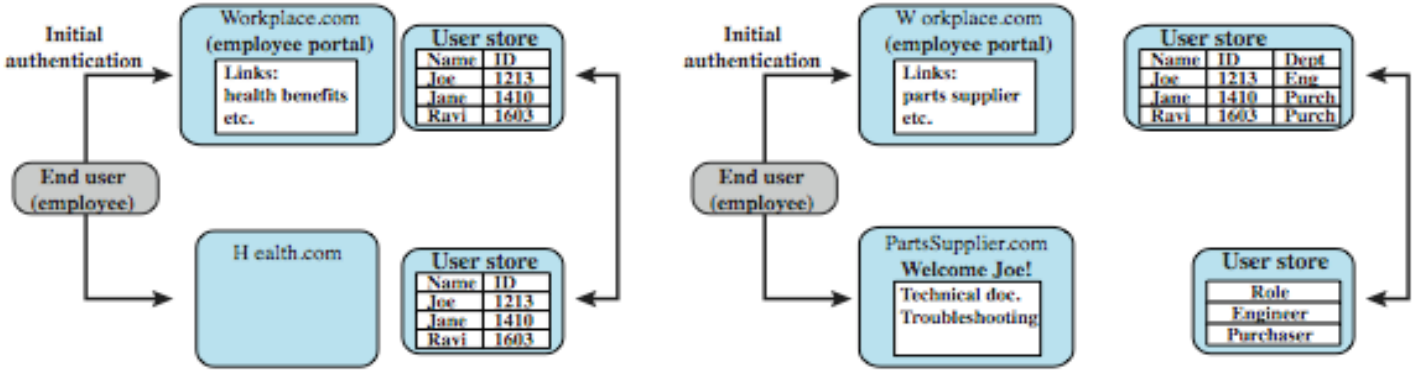
Process where authentication and permission will be passed on from one system to another, usually across multiple enterprises, reducing the number of authentications needed by the user.

Kerberos contains many of these elements

Identity Management*

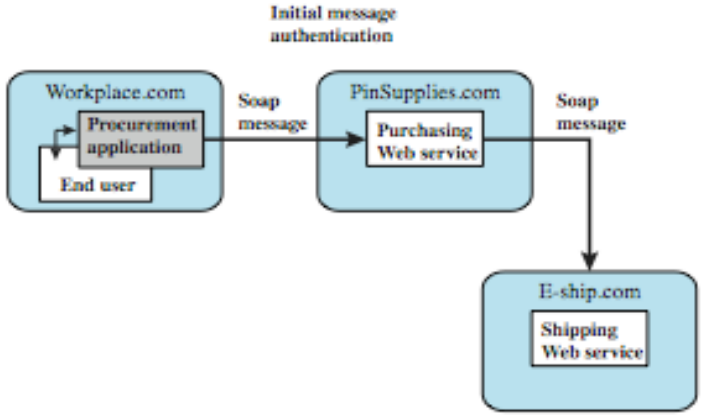


Federated Identity Management*



(a) Federation based on account linking

(b) Federation based on roles



Standards Used in FIM

Extensible Markup Language (XML)

characterizes text elements in a document on appearance, function, meaning, or context

Simple Object Access Protocol (SOAP)

for invoking code using XML over HTTP

WS-Security

set of SOAP extensions for implementing message integrity and confidentiality in Web services

Security Assertion Markup Language (SAML)

XML-based language for the exchange of security information between online business partners

Examples of FIM Initiatives

Some states in the U.S. are bringing up FIM systems with the goal of handling all state business

e.g., California, North Carolina

Microsoft .Net Passport

Shibboleth

Liberty Alliance

Microsoft .Net Passport

Centralized identity management architecture

Manage unique IDs with every user

No need to for remembering multiple Ids and passwords

No special infrastructure is required

Shibboleth

Internet2

Cloud computing

V 2.4.3 is the latest stable version (6 July 2011)

Does neither authentication nor authorization itself

Conveys security assertions from Identity Provider (IdP) to Service Provider (SP)

Identity is not necessary; attributes of person may be enough

Library Access

e.g., U of Texas System

Collaboration

Liberty Alliance

Multinational, multi-industry consortium

Over 150 companies, non-profit and government organizations

from around the world

Open standards for federated network identity

Extends security assertion markup language (SAML) to include additional security enhancements such as

Opt-in account linking

Simple session management

Global log-out capability

SAML is a XML based security standard that provides a way of exchanging user authentication information

Liberty Alliance

Enable consumers to protect the privacy and security of their network identity information

Enable businesses to maintain and manage their customer relationships without third-party participation

Don't need Certificate Authorities

Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers

Example

Airline, hotel and car rental federation

Summary

Passwords

Strong secure passwords, S/Key

PPP schemes

PAP, CHAP, EAP

Third party authentication systems

Kerberos, TACACS+, RADIUS

Mutual authentication

Digital certificates

Tokens

Biometric authentication

Multifactor authentication

Federated Identity Management

Some other schemes