UnitelmaSapienza
Università degli Studi di Roma

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Identification and Authentication 2

Prof. F. Parisi Presicce

Why Authentication?

- Common policy requirement: restrict the behavior of a user
  To permit different users to do different things, we need a way to identify or distinguish between users
  - Identification mechanisms to indicate/provide identity
  - Authentication mechanisms to validate identity
- When logging on to a computer you enter
  - user name and
  - password
- The first step is called identification:
  - You announce who you are.
- The second step is called authentication;
  - You prove that you are who you claim to be.

User Authentication

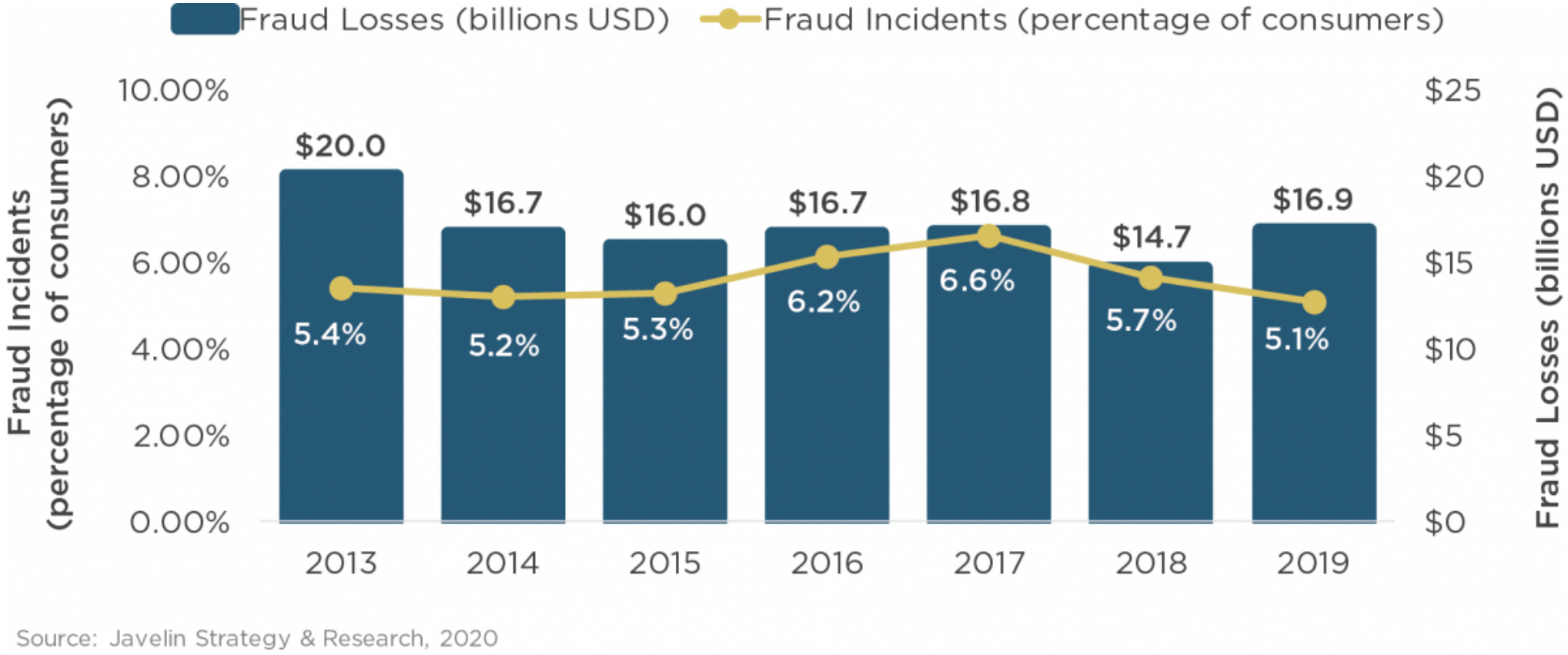
Common mechanisms for “proving” user identity

- where the user is
  - access to the keyboard or IP address
- what the user knows
  - passwords, personal information
- what the user possesses
  - a physical key, a ticket, a passport, a token, a smart card, a badge
- **what the user is (biometrics)**
  - **fingerprints, voiceprint, signature dynamics**
- … or some combination of these

Problems with Possession- or Knowledge-based Approaches

- Card may be lost, stolen or forgotten
  - Password or PIN may be forgotten or guessed by the imposters
- ~25% of people seem to write their PIN **on** their ATM card
- Estimates of annual identity fraud:
  - More than 11 million adults became victims of identity fraud in 2011
  - $1 billion in fraudulent cellular phone use
  - $3 billion in ATM withdrawals
- The traditional approaches are unable to differentiate between an authorized person and an impostor

Estimates of annual identity fraud



Source: Javelin Strategy & Research, 2020

- Javelin Strategy & Research, 2020 Identity Fraud Report

“Something about you”

- Biometrics are increasingly common as identification rates improve.
  - fingerprints
  - retinal scan, iris scan
  - facial heat
  - voice pattern/recognition
  - signatures (handwriting)
  - typing
- See also:
  - U.S. National Biometric Test Center; San Jose State Univ. (CA)
  - www.nist.gov/biometrics

What are Biometrics?

- **Biometrics** – science, which deals with the automated recognition of individuals (or plants/animals) based on biological and behavioral characteristics
  - Identification or verification
- **Biometry** – mathematical and statistical analysis of biological data
- **Biometric system** – a pattern recognition system that recognizes a person by determining the authenticity of a specific biological and/or behavioral characteristic (biometric)
- **Anthropometry**–measurement techniques of human body and its specific parts
- **Forensic (judicial) anthropometry**–identification of criminals by these measurement techniques

Biometrics is Not New!!

- Bertillon system (1882) took a subject's photograph, and recorded height, the length of foot, arm and index finger
- Galton/Henry system of fingerprint classification adopted by Scotland Yard in 1900
- FBI set up a fingerprint identification division in 1924
- AFIS installed in 1965 with a database of 810,000 fingerprints
- First face recognition paper published in 1971
- FBI installed IAFIS in ~2000 with a database of 47 million prints; average of 50,000 searches per day; 2 hour response time for criminal search

Emphasis now is to automatically perform reliable person identification in unattended mode, often remotely (or at a distance)

Requirements for an Ideal Biometric Identifier

1. Universality
   – Every person should have the biometric characteristic
2. Uniqueness
   - No two persons should be the same in terms of the biometric characteristic
3. Performance
   - The biometric characteristic should be invariant over time
4. Collectability
   - The biometric characteristic should be measurable with some (practical) sensing device
5. Acceptability
   - One would want to minimize the objections of the users to the measuring/collection of the biometric

Identifiable Biometric Characteristics

- **Biological traces**
  - DNA, blood, saliva,etc.
- **Biological (physiological) characteristics**
  - fingerprints, eye irises and retinas, hand palms and geometry, and facial geometry
- **Behavioral characteristics**
  - dynamic signature, gait, keystroke dynamics, lip motion
- **Combined**
  - voice

Biometrics

2 Categories of Biometrics

- **Physiological** – also known as static biometrics: Biometrics based on data derived from the **measurement of a part of a person's anatomy,** e.g., fingerprints and iris patterns, facial features, hand geometry and retinal blood vessels
- **Behavioral** – biometrics based on data derived from **measurement of an action performed by a person**, indirectly measuring human characteristics. Essential to incorporate time, e.g. voice (speaker verification), signature

Using Biometrics

Process flow includes enrollment, and verification/identification.

- Enrollment
  - Person entered into the database
  - Biometric data provided by a user is converted into a template.
  - Templates are stored in a biometric systems for the purpose of subsequent comparison.
  - Size of template quite large compared with password, and not directly related to accuracy
- Verification: Are you who you claim to be?
  - One to one comparison: confirm or deny the specific identification claim of a person.
- Identification: Who are you?
  - One to many comparison: determine identity of a person from biometric database without the person first claiming identity.

Verification and Identification

Verification system answers the question: “Are you who you claim to be?”

- The answer returned by the system is *match* or *no match* (in biometric systems a score, which may indicate inconclusive)
- Identification system requires more computational power than verification systems, and has more opportunities to err.

Identification systems answers the question: “Who are you?”

- The answer returned by the system is *an identity (name or ID number).*

Some typical biometrics

- Primarily Physical Features
  - Hand based
    - Fingerprint or finger-scan
    - Hand geometry
  - Face/eye
    - Facial recognition
    - Retinal scans / Iris scans
- Strong Behavioral Component
  - Voice recognition
  - Signature recognition, including how the signature is produced (pressure, speed, stroke order) and not just how the signature looks
  - Typing style, including speed and rhythm of key pressure

Forged Fingers

- Fingerprints, and biometric traits in general, may be unique but are no secrets.
- we leave fingerprints in many places.
  - http://www.ccc.de/updates/2008/schaubles-finger (in German)
- Rubber fingers have defeated many commercial fingerprint recognition systems in the past.
  - Minor issue if authentication takes place in presence of security personnel.
  - When authenticating remote users, additional precautions taken to counteract this type of fraud.
- User acceptance: so far fingerprints have been used for tracing criminals.

Other Characteristics

Can use several other characteristics

- Eyes: patterns in irises unique
  - Measure patterns, determine if differences are random; or correlate images using statistical tests
- Faces: image, or specific characteristics like distance from nose to chin
  - Lighting, view of face, other noise can hinder this
- Keystroke dynamics: believed to be unique
  - Keystroke intervals, pressure, duration of stroke, where key is struck
  - Statistical tests used at enrollment

How does this work?

Some aspects are quite similar to standard authentication procedures information

- Calibrate and store user
  - Storage styled vary: 20 years ago, common to encrypt bio info and store it; alternatively, store a validator (hash) of the information. Now templates are used (sometimes several times) at enrollment.
- Authenticate “as usual”:
  - user ‘inputs’ biometric information (may not be overt and may not be single event) and then proceed by matching verification template with stored template.

Devices Usually Required

- The device collecting the data is often proprietary and/or uses proprietary algorithms
- Patents protect much of the technology
- There may be considerable computation involved in computing a “validator” or template for storage (far beyond the Unix validator)
- Sometimes the biometric requires local installation of a specialized reader device (such as for fingerprints, but not for voice)

Matches are probabilities

Identifying information is not typed in, but obtained by a device (imprecise measurement)

- Characteristics mapped from analog to digital and not all of the original information is retained
- Devices for most common biometrics may not produce identical results or even identically repeatable results
  - Ex: fingerprint readers depend on environmental factors such as the positioning of the finger, the “moisture” of the hand, oils, and occupational issues which may cause a print to be roughened over time

Effectiveness

- Two types of errors for Authentication
  - False Acceptance (FA)
    - Let imposters in
    - FAR : probability that an imposter is authenticated
  - False Rejection (FR)
    - Keep authorized users out
    - FRR : probability that an authorized user is rejected
- Another type of error for identification
  - False Match (FM)
    - One user is mistaken for another (legitimate) user
    - FMR : probability that a user is incorrectly matched to a different user's profile
- No technique is perfect

Equal-error Rate

- By setting matching threshold (FAR=FRR), trade off lower false acceptance rate against higher false rejection rate, and vice versa.
- Finding right balance between those two errors depends on application.
- Equal error rate (EER): given by threshold value where FAR=FRR .
- Currently, best state-of-the-art fingerprint recognition schemes have EER of about 0.5 - 2%.
- Iris pattern recognition has a superior performance.
- http://bias.csr.unibo.it/fvc2006/

How you do it

- People perform mechanical tasks in way both repeatable and specific to individual.
- Experts look at dynamics of handwriting to detect forgeries.
- Users could sign on special pad that measures attributes like writing speed pressure.
- On keyboard, typing speed and key strokes intervals used to authenticate individual users.

Multimodal Biometrics

Use multiple biometrics together

- AND : accept only when all checks are successful
- OR : accept as long as one is successful
- other possible combinations

Any of these can be fooled!

- Assumes biometric device accurate *in the environment it is being used in!*
- Transmission of data to validator is tamperproof, correct

Identity

Authentication is the binding of an identity to a subject

But what is identity?

- A set of properties/attributes characteristic of a principal (subject or object)

How to represent identity?

- randomly chosen : not useful to humans
- user chosen: probably not unique globally
- hierarchical system: used to disambiguate
  - file system
  - X.500
  - IP address

Anonymity

What if identity not needed?

- Web browsing
- Complaints about assignments

Removing identity not as easy as it sounds

- I can send email without my userid
- But it still traces back to my machine

Solution: anonymizer

- Strips identity from message
- Replaces with (generated) id
- Send to original destination
- Response: map generated id back to original identity

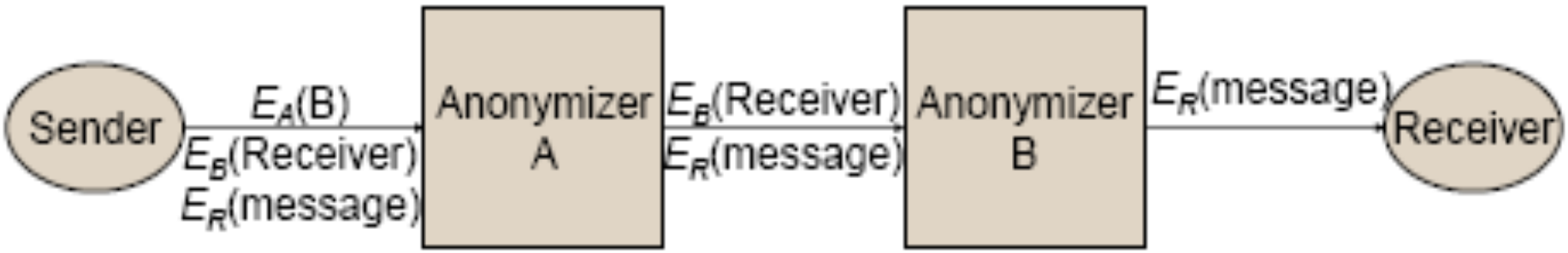
Anonymity

Problem: Anonymizer knows identity

- Can it be trusted?
- Courts say no!

Solution: multiple anonymizers

- Onion Routing
- Crowds



Key Points

- Authentication is not (precise as) cryptography
- Passwords will still be used
  - provide a basis for most forms of authentication
- Protocols used are important
  - making masquerading harder
- Authentication methods can be combined
- Hiding Identity, instead of verifying it, is sometimes preferable
  - https://ifip-summerschool2021.uni.lu/