TDDE49 Databases Topic 7: Information security concepts

Matus Nemec
matus.nemec@liu.se
VT2 2021

LINKÖPING UNIVERSITY

Recommended literature

- **Computer Security and the Internet**
  - by Paul C. van Oorschot; first edition (2020)
  - https://people.scs.carleton.ca/~paulv/toolsjewels.html
  - Full text via LiU library: https://liu.se/en/library
- **Security Engineering** by Ross Anderson
  - Second edition (2008) is free from the author
  - https://www.cl.cam.ac.uk/~rja14/book.html
  - Third edition (2020) in LiU library (not online)
- **Threat Modeling** by Adam Shostack
  - 2014, in LiU library, online access for students

Information security goals

Information security goals

- Typically **defense** against **intentional** misuse
- Unathorized malicious actions and their consequences
  - Prevention of such actions
  - Detection and recovery from attacks
- Main goals: confidentiality, integrity, availability

- Attacker is often a few steps ahead – unknown threats
- Protection against unintentional damage and modification also a requirement, but not the focus of computer security
  - E.g., reliability and redundancy

Confidentiality

- Goal: limiting access to non-public information, data is made available only to authorized users
- Stored and transmitted data is not revealed to unapproved (unauthorized) users

- Loss of confidentiality consequences:
  - Unauthorized data disclosure can lead to loss of trust in the organization, legal liability, fines, etc.
  - Example: Medical records available on the public Internet
- Technical means of protection:
  - Data encryption, access control

Integrity

- Goal: accuracy and completeness of information
- Protection against unauthorized data modification

- Loss of integrity consequences:
  - Data is no longer valid (reflecting reality) and reliable
  - Example: A patient changes their prescription
- Technical means of protection:
  - Message authentication codes, secure hash algorithms
  - Error detection/correction codes can be easily recomputed and **do not** protect against malicious data modification
  - So are outdated hash algorithms insufficient: MD5, SHA-1

Availability

- Goal: the system is accessible by authorized users when needed
- Protection against unauthorized deletion of data and disruption of services

- Loss of availability consequences:
  - Loss of productivity, inability to reach business goals
  - Example: A doctor cannot read patient's past diagnoses
- Technical means of protection:
  - Denial of Service (DoS) protection
  - Reliability and redundancy, backup and recovery

Related goals and concepts

- Privacy
  - Confidentiality of personally sensitive information
- Authenticity of data
  - Integrity of origin – the author of the data is reliably known
- Accountability (and audit)
  - Ability to assign responsibility for past actions
  - E.g., transaction log of actions and identities
- Non-repudiation
  - Actions and commitments cannot be denied (repudiated)
  - E.g., cryptographic signature (limited access to signing keys)

Information security goals (CIA) summary

- Confidentiality
  - Only authorized users can access the non-public information
  - Data in storage and transit is not undesirably revealed
- Integrity
  - Accuracy and completeness of information
  - Data remains unaltered, except by authorized users
- Availability
  - The system is accessible by authorized users when needed
  - Protection against unauthorized deletion and disruption
- Sometimes includes Accountability and Non-repudiation
  - Actions attributed to users who cannot deny responsibility

Access control

Access control

- Restricts access to resources to authorized users
- Enables auditing of actions
- Possible implementation – access control list (ACL)
  - Each system resource (object) is assigned a list of permissions
  - Each list specifies which users (subjects) have access to the object and what operations are allowed on the object
  - Example: filesystem of an operating system
  - Users can be assigned to groups

Role-based access control (RBAC)

- Authorization can be based on a role; each role is assigned permissions, roles are assigned to users
  - E.g., teacher in a course X can give final grades for course X
  - Easier to assign a single role to a user than to manage the same set of permissions repeatedly for many users
  - Easier to manage the permissions of a role than to change the same permission repeatedly for many users
- Users can have multiple roles or groups
- RBAC also enables auditing of actions
  - Accountability is based on identity
  - Group accountability is ineffective

Access control procedure

1. Identification – Making a claim about someone's identity
   - E.g., stating your name; presenting a username to a website
2. Authentication – Verification of a claim of identity
   - E.g., comparing a photo on your ID card to your face; checking if a username and a password match
3. Authorization – Determining the permitted actions
   - E.g., which features are accessible
   - Defined by policies (e.g., only the system administrator is allowed to install new programs), enforced by access control mechanisms (e.g., file system permissions: read, write, execute)

User authentication

User authentication

- Verification of a claim of identity
- Allows making access control decisions: authorization

1. Something you know
   - E.g., a password, a PIN, an answer to a security question
2. Something you have
   - E.g., the LiU card, a credit card, a key to your apartment
3. Something you are
   - Biometrics, e.g., based on fingerprint/iris/face recognition

- Something you do – behavior (handwriting, voice recognition, …)
- Where you are – location based authentication (e.g., geolocation)

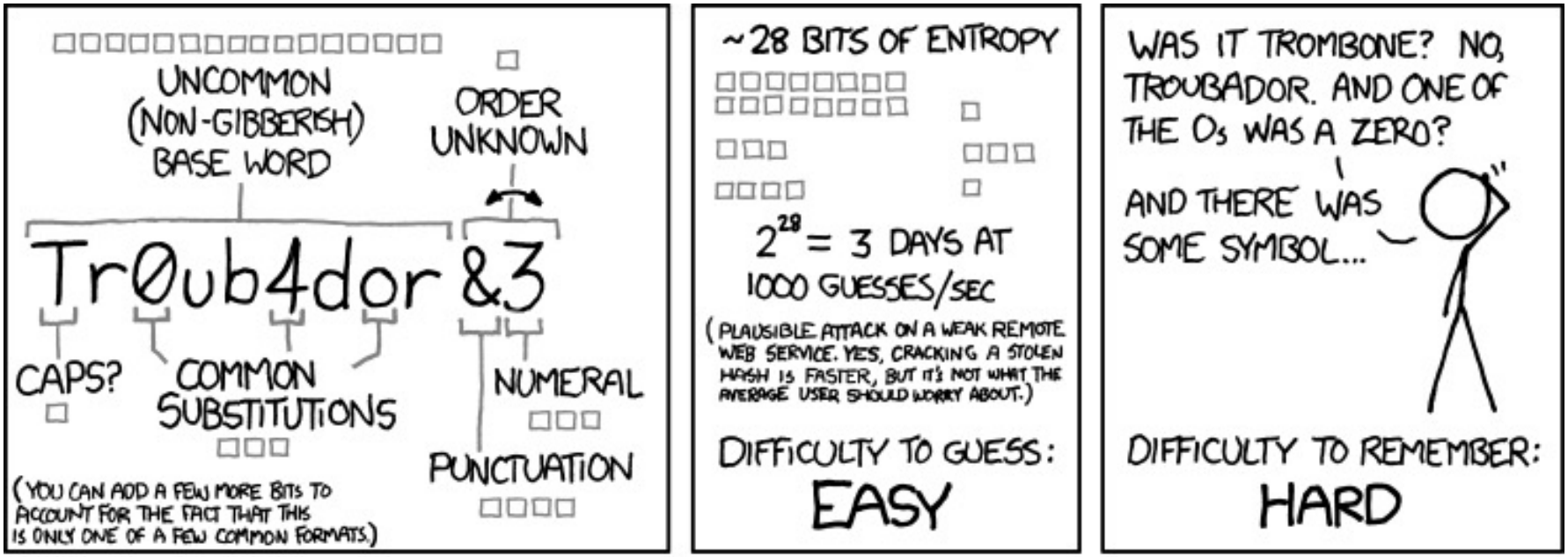
Something you know – passwords 1/2

- Typical account with a **username** and a **password**
- Some advantages:
  - Easy to use and understand
  - No extra device required – no extra cost
  - Easy to change or recover if lost
  - Quick (especially with password managers)
  - Easy to delegate (although users may forget to change the password to take back the delegation)
  - Well studied (user behavior, attacks)

Something you know – passwords 2/2

- Password disadvantages – usability issues:
  - Password re-use across accounts is insecure
  - Do not write down your password
  - Make it easy to remember, but difficult to guess
  - Complicated policies – length, special characters
  - Expiration policies (e.g., change every 90 days) – outdated and counterproductive
- E.g., LiU tips on passwords: https://insidan.liu.se/it/it-sakerhet/tips-for-ett-sakert-losenord?l=en
- Look for more resources before you implement!

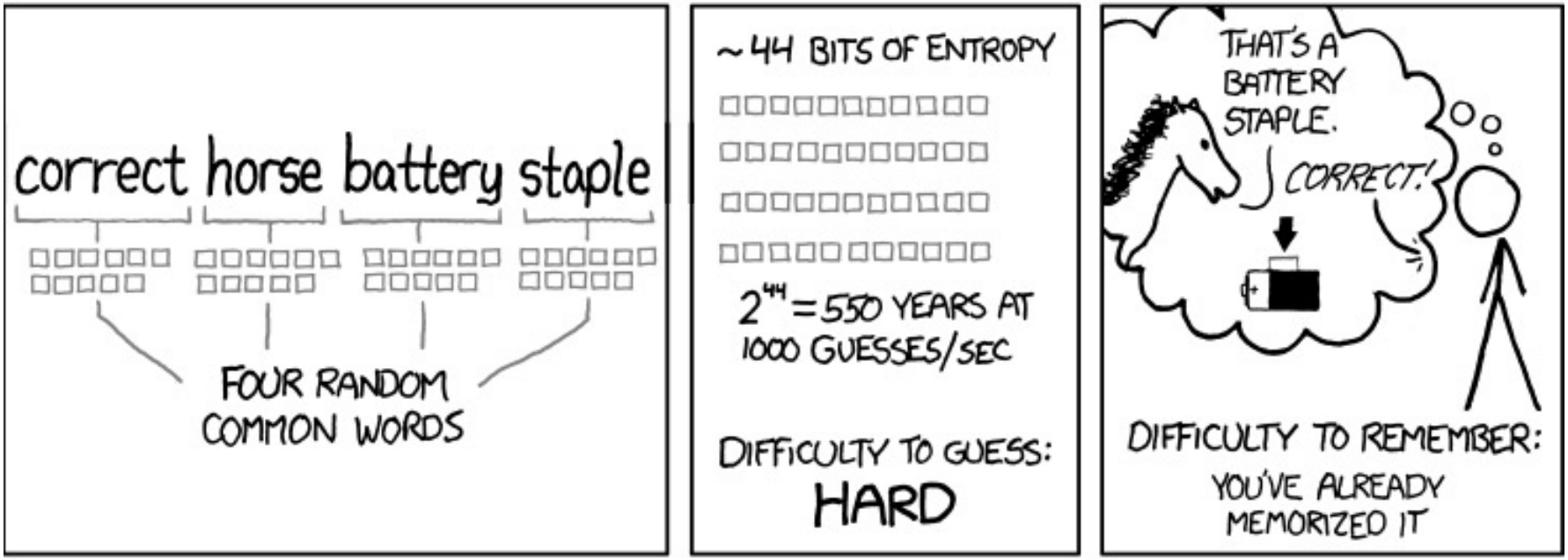
Trouble with passwords



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

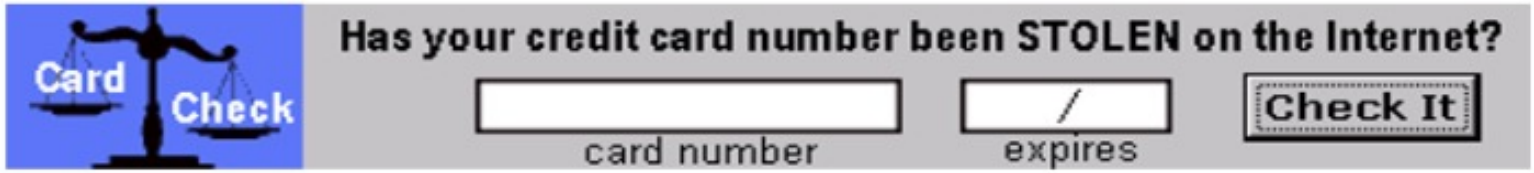
https://xkcd.com/936/

An option for choosing a password

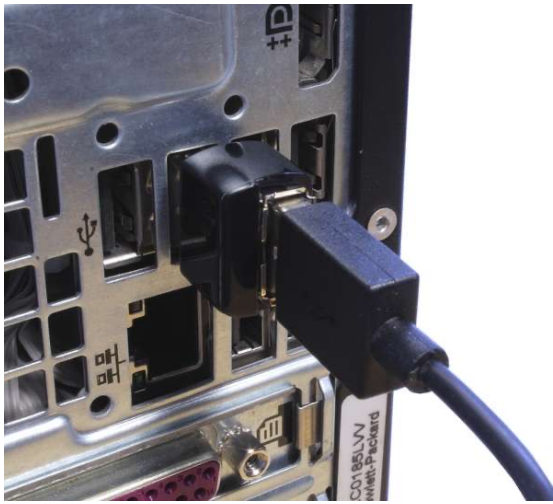


https://xkcd.com/936/

Password stealing



- Phishing: asking users to log in under false pretense
- Spoofing: genuine-looking fake URL, login screen
- Social engineering: targeted attacks
- Malware: keyloggers; also physical ->
- Physical access: shoulder surfing
- Password reuse: Have I Been Pwned?
  - https://haveibeenpwned.com/



A case for password managers

- Phishing is getting better and difficult to detect
  - Attackers use TLS encryption (“green lock”) and other tricks
  - Example: internationalized domain name (IDN) homograph attack; the Latin letters “e” and “a” are replaced with the Cyrillic “e” and “a”: wikipedia.org
  - A password manager automatically fills in the password only at the genuine website
- Secure passwords are difficult to remember
  - A password manager generates a unique random one
- Open-source options, e.g., KeePass: https://keepass.info/
  - Beware of fakes, e.g., keepass (dot) com

Something you have

- Keys, badges, tokens, smart cards
- Can be lost, stolen
  - Difficult (costly) to replace, but loss can be quickly detected
- Some can be copied
  - E.g., credit card skimming – copy of the magnetic stripe; radio eavesdropping on RFID key cards; some car keys
- Cryptographic smartcards have more abilities (mobile phone SIM, credit card, also in ID cards, passports, …)

<- RFID card
Photo Peter Modin

ID with a cryptographic Smartcard ->
Photo by Skatteverket

Something you have – tokens

- Devices that produce one time passwords (OTP)
- Can offer strong cryptography and cannot be copied
  - Often extremely difficult to copy even with physical access
- Cryptographic functions with a secret key applied to a unique challenge and/or the current time
- Challenge-response token (e.g., bank token)
- Time-based token (e.g., RSA SecurID)
- Still vulnerable to phishing

By I. Hölscher

By A. Klink

Something you have – web authentication

- Tokens that support various web standards
  - Universal 2nd Factor (U2F), FIDO2
  - One-time Password (OTP) algorithms
  - Digital signatures, e-mail encryption, etc.
  - Communicate via USB or NFC (Near-field communication)
- E.g., SoloKey, YubiKey
- Can be costly (20 to 60 EUR)

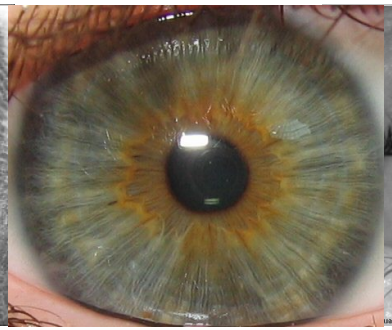
SoloKeys

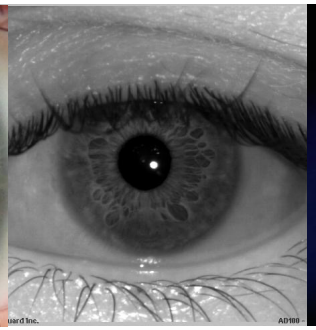
YubiKey

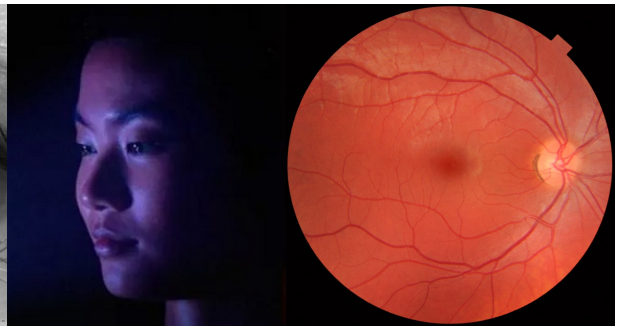
Something you are – biometrics 1/3

- Using biological properties for identification
- Identification vs. verification of identity
  - Identification – identify a user from all possible users
  - Verification only – e.g., in a combination with a user ID/PIN
- Fingerprint, iris (visible/infrared light), face, retina


By M. Goldthwaite


By J. Daugman


By Apple


By M. Häggström

Something you are – biometrics 2/3

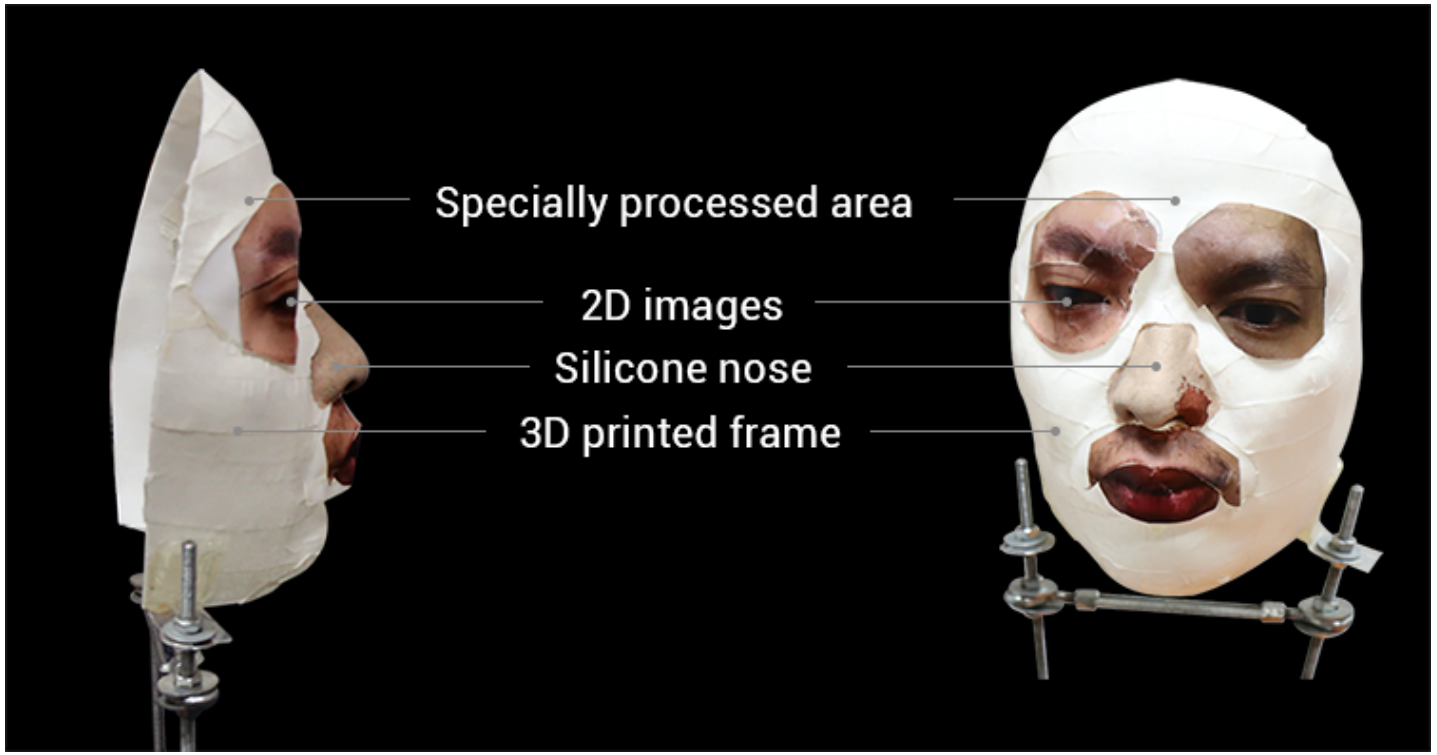
- Advantages
  - Usability – nothing to carry, no cognitive burden
  - Cannot be forgotten
- Some challenges and disadvantages
  - Variable (slightly different each time you measure)
  - Not secret and easily acquired, yet also cannot be changed
  - Failure to enroll – some users cannot use the method easily
  - Failure to capture – e.g., cannot be read with wet fingers
  - Requires a fallback mechanism for such cases
  - Can falsely reject legitimate and falsely accept ilegitim. users

Something you are – biometrics 3/3

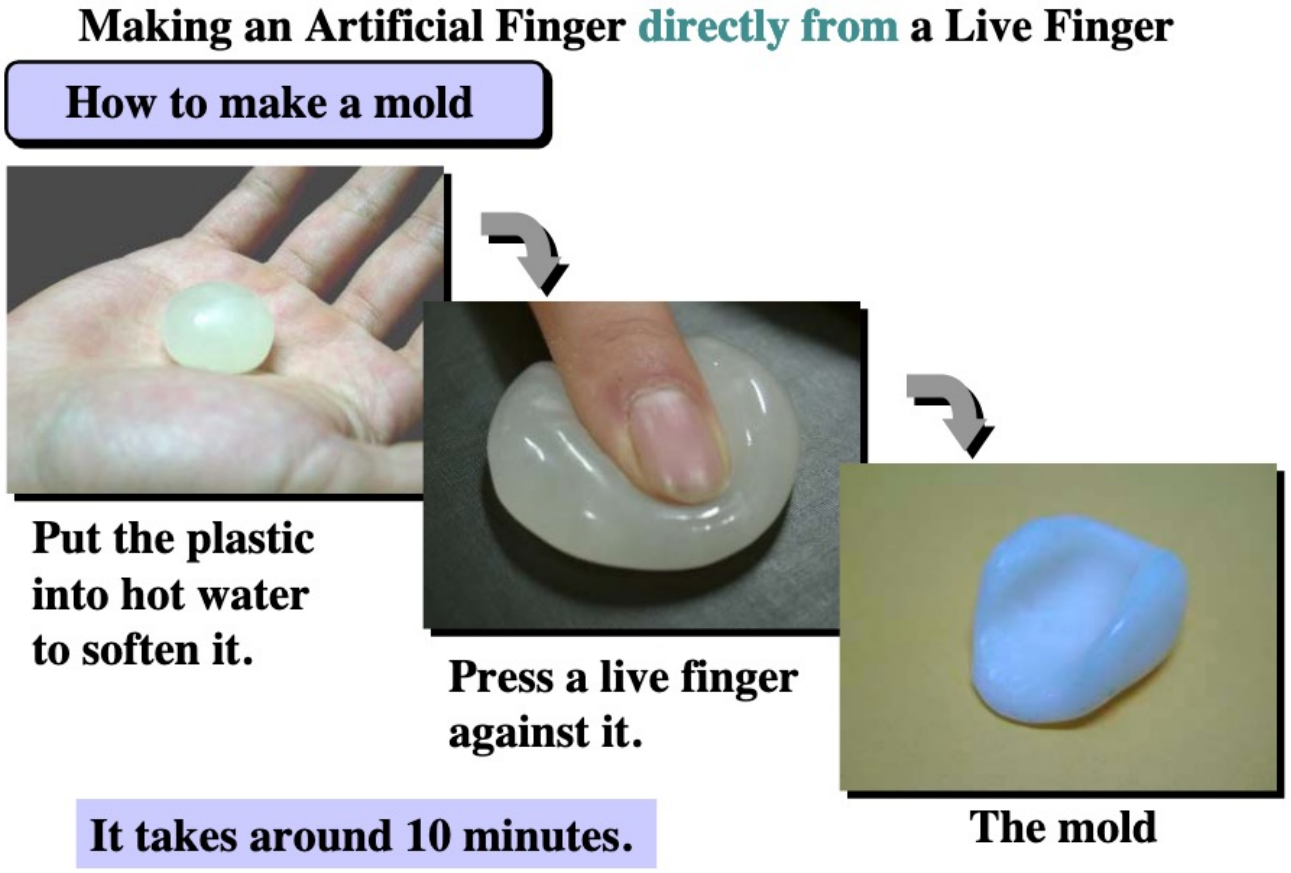
- Requirements for biometrics
  - Unique – The property is distinct for different individuals
  - Permanent – The property cannot change over time
  - Universal – Almost everyone has such property
  - Collectable – It is possible to easily measure the property
  - Difficult to circumvent – Hard to fool the system
- In summary, biometrics are suitable as an additional (second factor) authentication or used under supervision (e.g., security checkpoint)

Fooling biometrics

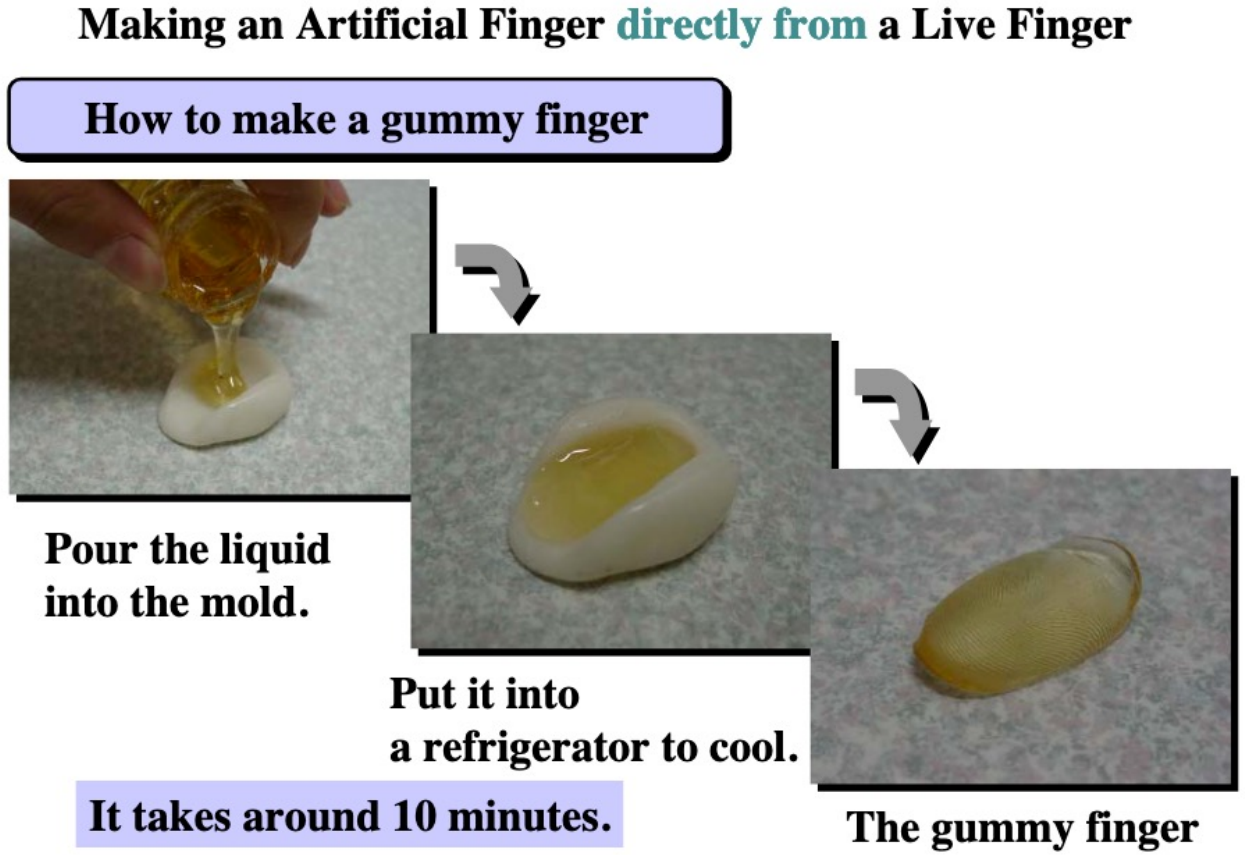
- 3D-printed mask for FaceID on an iPhone X in 2017 by BKAV



Fooling biometrics – Tsutomu Matsumoto 1/2

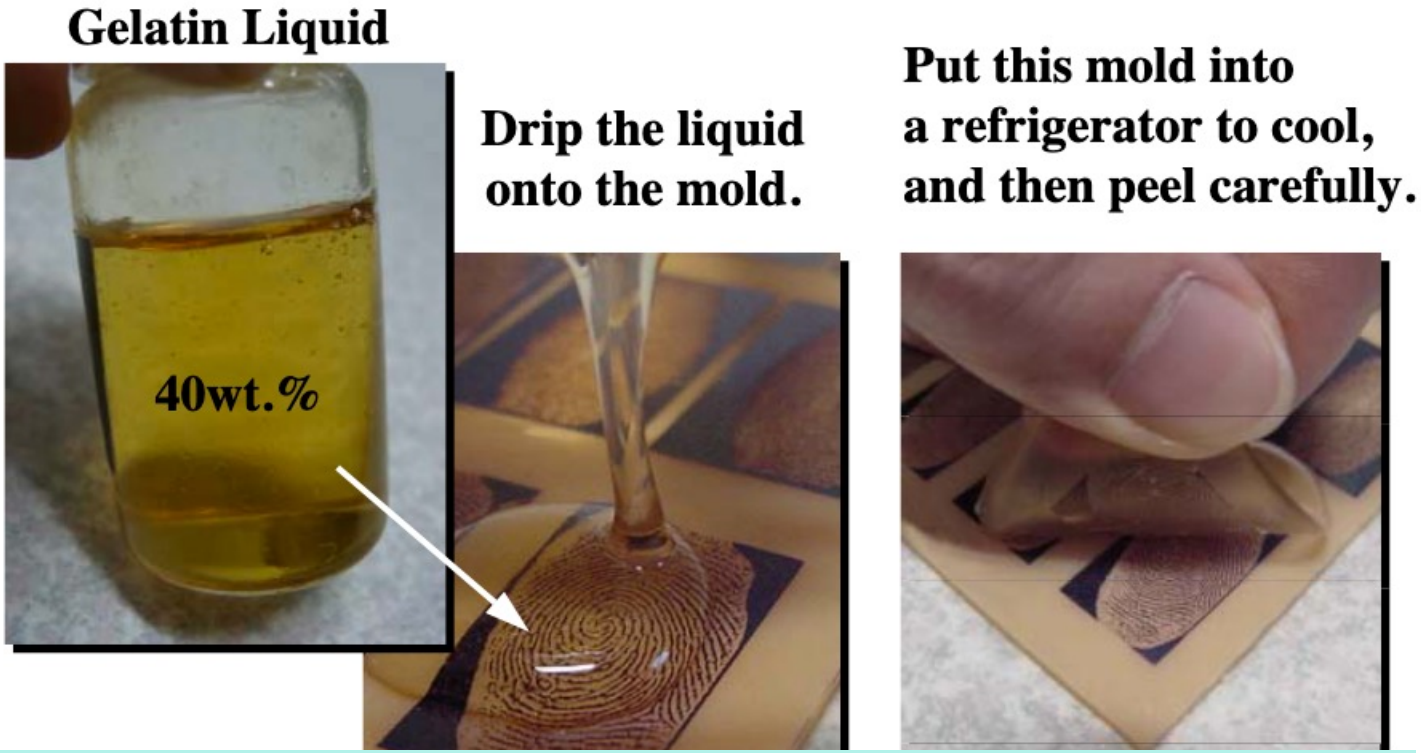


Fooling biometrics – Tsutomu Matsumoto 2/2



- Attack from 2002, can be defeated by a liveness check

Fooling biometrics – fake fingerprints



- Fingerprint image, laser printer, glue; fools optical fingerprint reader; Tsutomu Matsumoto 2002

Multi-factor authentication

- Two methods used in parallel
- Typically from different categories (not 2 passwords)
- Examples:
  - Password and a one-time PIN received via SMS/from a challenge-response calculator/from a push notification
  - Payment terminals, ATM – chip-card and a PIN
  - Password and a biometric
- Mandatory with payment service providers in the EU
- Easy to setup with phone apps for web services
  - (e.g., OTP with Google, Microsoft authenticator)

User authentication summary

- Verification of identity using different methods:

1. Something you know
   - E.g., a password, a PIN, an answer to a security question
2. Something you have
   - E.g., a passport, BankID, token device (“bankdosa”)
3. Something you are
   - Biometrics, e.g., based on fingerprint/iris/face recognition

- Multi-factor authentication (MFA, 2FA for 2-factor auth.)
  - E.g., password and a one-time password from a device


LINKÖPING
UNIVERSITY