

# TDDE49

## Information security concepts

Ulf Kargén

ulf.kargen@liu.se

# 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
- Unauthorized 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  - Data is no longer valid (reflecting reality) and reliable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 is able to change their own prescription
- Technical means of protection:
  - Message authentication codes, secure hash algorithms

# 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:
  - 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)



# 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

# Role-based access control (RBAC)

- Authorization can be based on a role; each role is assigned permissions, roles are assigned to users
  - 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

## Example:

1. The *manager* role has access to personnel files, but not to web server configuration.
2. *IT-admin* role has access to web configuration, but not to personnel files.

**But:** If *manager* and *IT-admin* is the same person, he/she has access to both

# 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)

# 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)



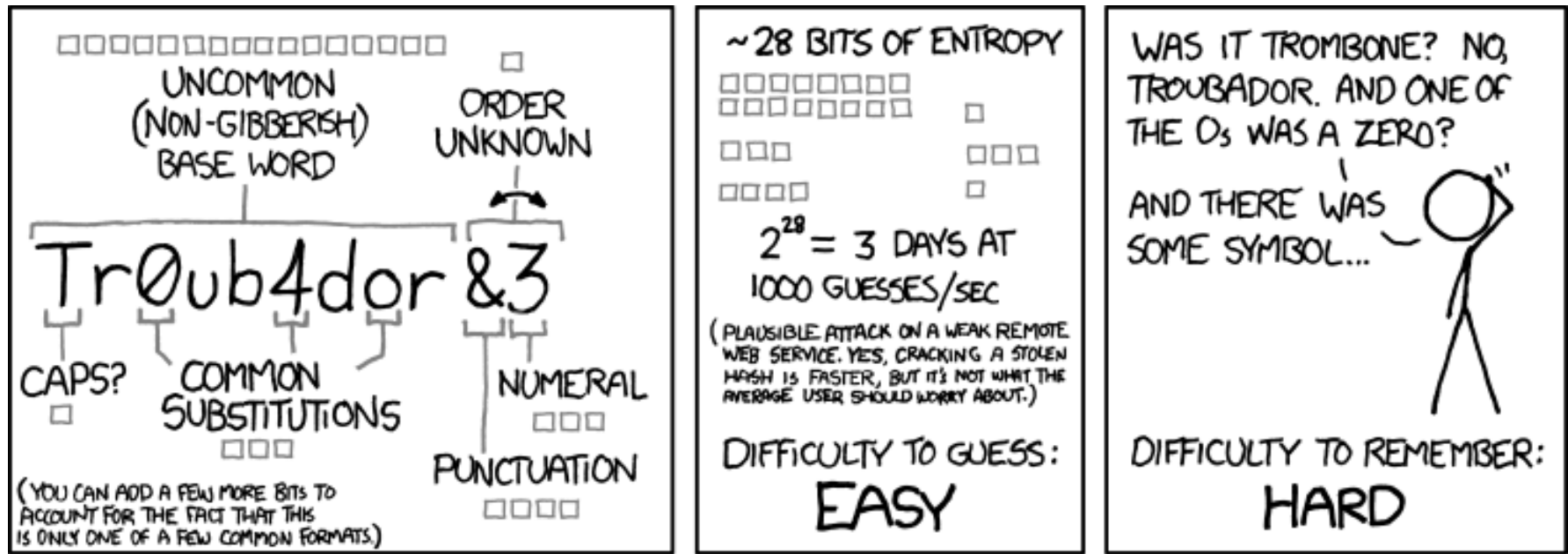
# Something you know – passwords 1/2

- 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**
    - Password is never more secure than the *least* secure site/system where you reused it!
  - Avoid writing 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

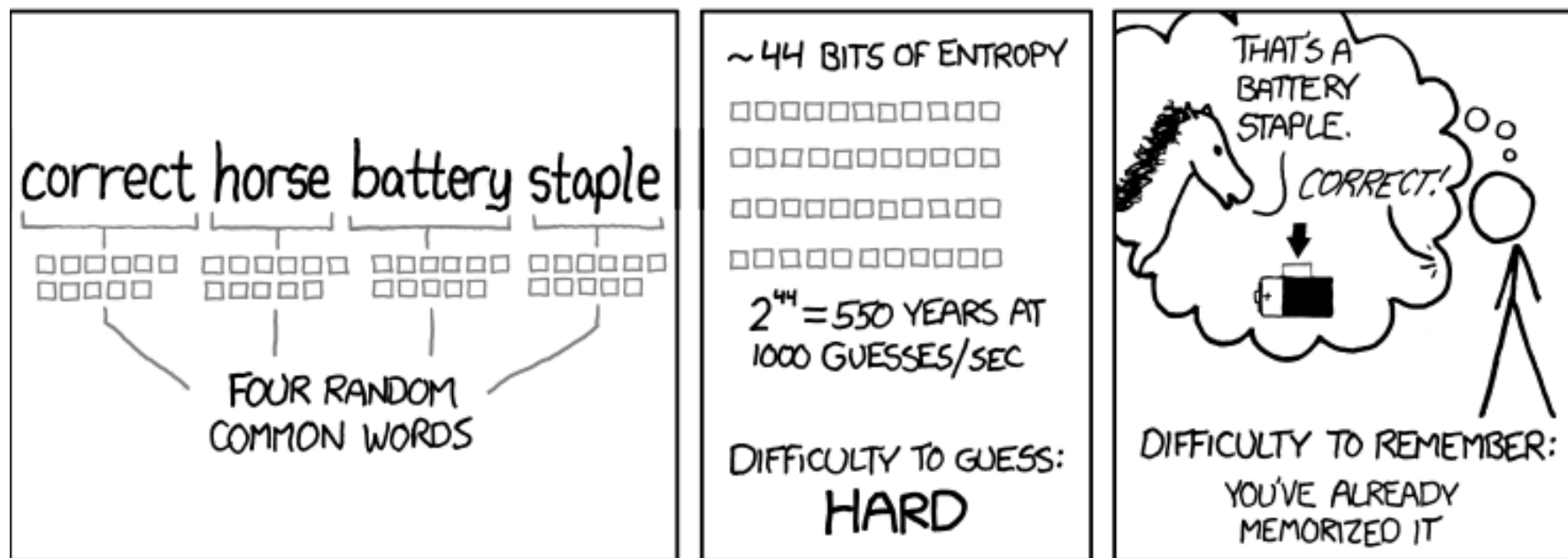
# Trouble with passwords



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/>

# 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



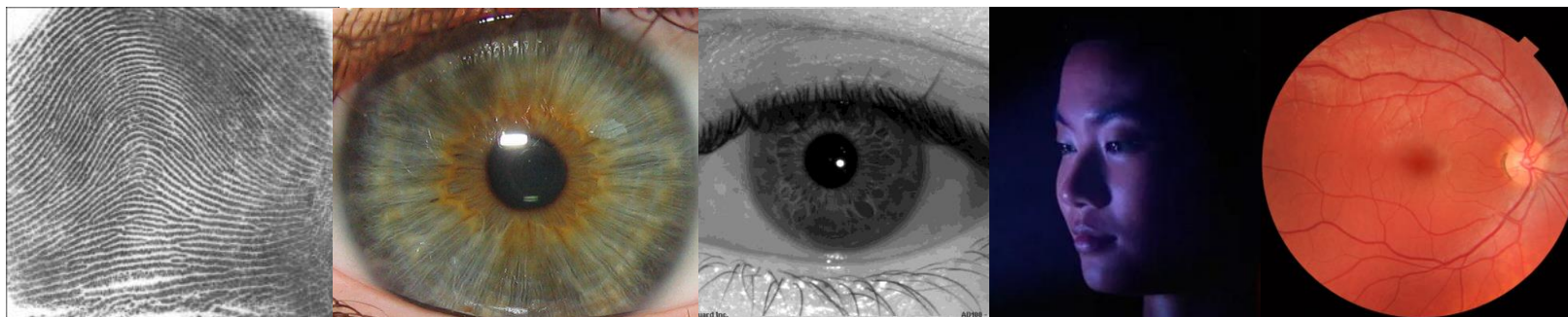
By I. Hölscher



By A. Klink

# Something you 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 illegitimate users

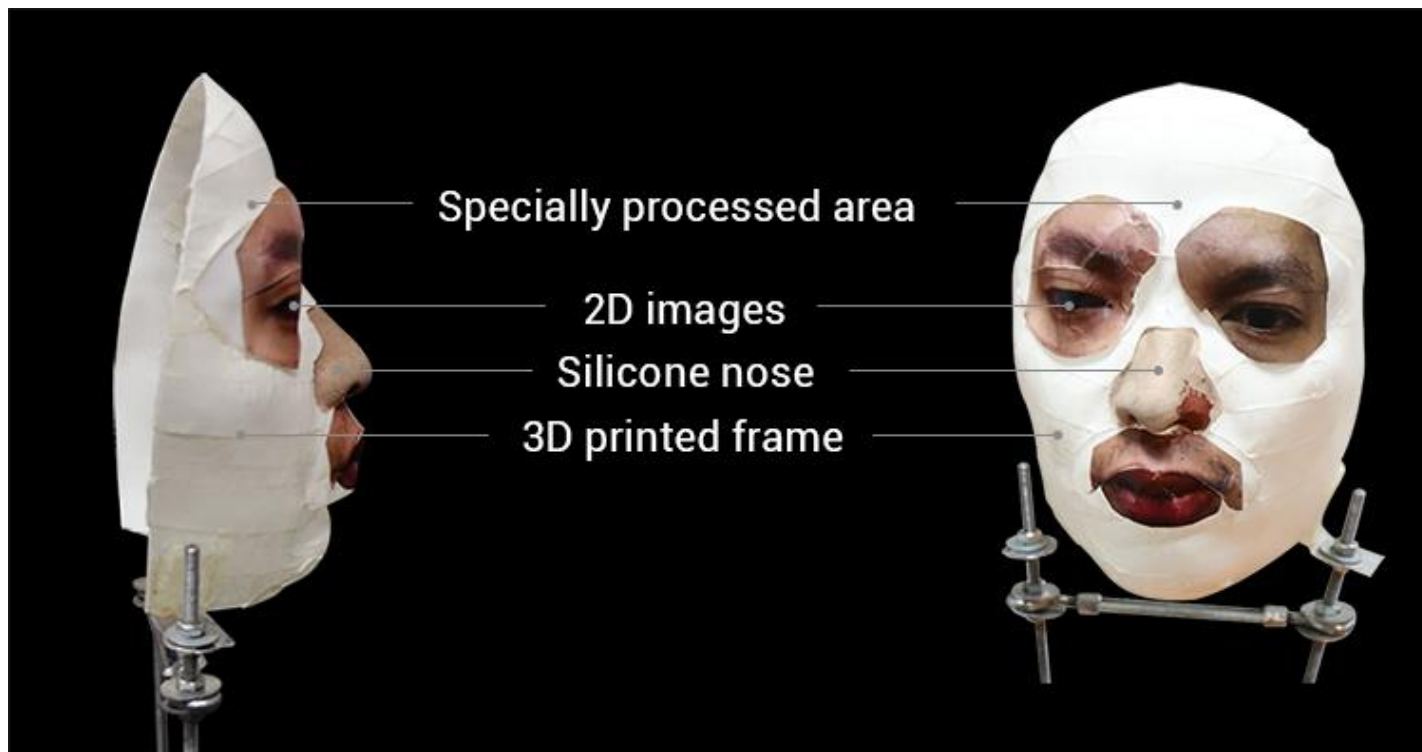


# Something you are – biometrics 3/3

- 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

Making an Artificial Finger **directly from** a Live Finger

How to make a mold



Put the plastic into hot water to soften it.



Press a live finger against it.



The mold

It takes around 10 minutes.

# Fooling biometrics – Tsutomu Matsumoto

## 2/2

Making an Artificial Finger **directly from** a Live Finger

### How to make a gummy finger



**Pour the liquid into the mold.**



**Put it into a refrigerator to cool.**



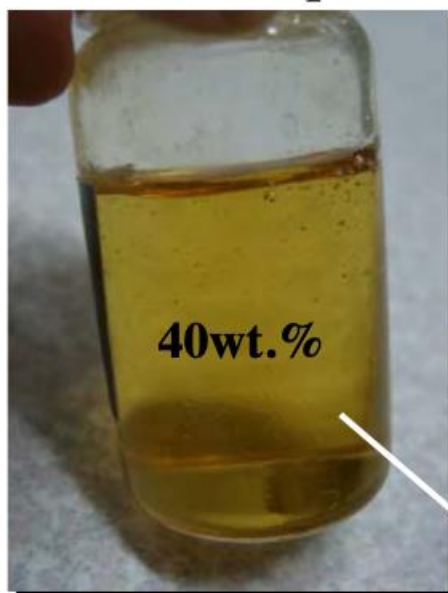
**The gummy finger**

**It takes around 10 minutes.**

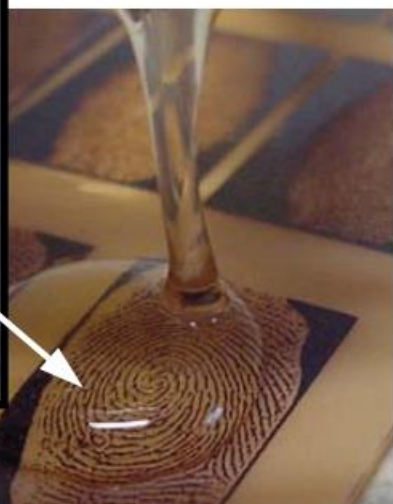
- Attack from 2002, can be defeated by a liveness check

# Fooling biometrics – fake fingerprints

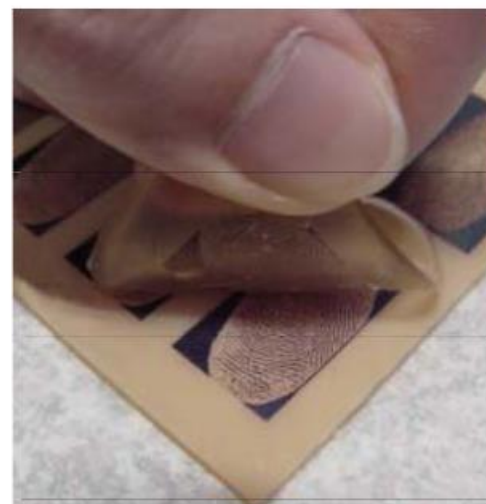
## Gelatin Liquid



**Drip the liquid onto the mold.**



**Put this mold into a refrigerator to cool, and then peel carefully.**



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

# 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

# Common attacks

# Know Thy Enemy

A few common attack scenarios (in no particular order):

1. Password attacks
  - a) Brute-force
  - b) Dictionary attacks
  - c) Credential stuffing
2. Social engineering – Phishing, Spear phishing
3. Malware – Ransomware, Spyware, etc.
4. Software exploits



# Password attacks – Brute force

- A **search attack** is the most basic form of brute force.
- Given a character set (e.g. [*abcdefghijklmnopqrstuvwxyz*]) and a password length, try every possible combination
- For example, lower case letters, 3 character password:
  - aaa
  - aab
  - aac
  - ...
- Slow, but it will at some point crack the password.

# Password attacks – Dictionary attacks

- **Dictionary attacks** exploit the fact that it is common for users to pick passwords that are easy to remember
  - The password “123456789ABC” is a lot more common than “frex#be!?Vu6adR”...
- Use a predetermined list of words (a dictionary) and try these as passwords
  - An actual dictionary of common words
  - Even better: A leaked set of real passwords

# Password attacks – Dictionary attacks



1. 123456	4.1%	11. login	0.2%
2. password	1.3%	12. welcome	0.2%
3. 12345	0.8%	13. loveme	0.2%
4. 1234	0.6%	14. hottie	0.2%
5. football	0.3%	15. abc123	0.2%
6. qwerty	0.3%	16. 121212	0.2%
7. 1234567890	0.3%	17. 123654789	0.2%
8. 1234567	0.3%	18. flower	0.2%
9. princess	0.3%	19. passw0rd	0.2%
10. solo	0.2%	20. dragon	0.1%

“Skyhigh analyzed 11 million passwords for cloud services that are for sale on Darknet...” (2015)

# Password attacks – Dictionary attacks

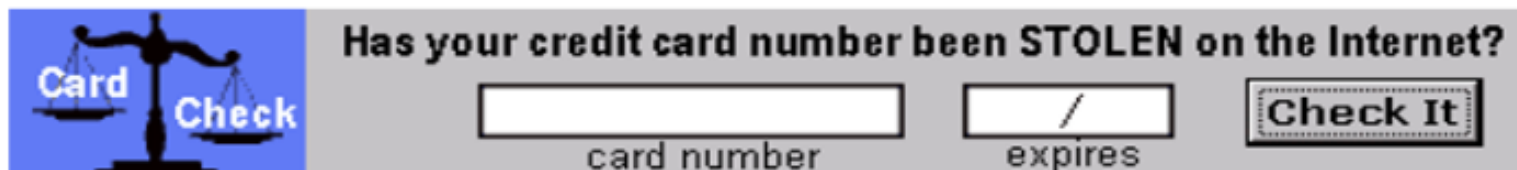
- **Rule-based search:** make up some transformation rules that you apply to each candidate password.
- Example: use the following transformations: ***duplicate, toggle case, replace e with 3***.
  - Assume we want to test the password: ***pressure***, then we would test:
    - *pressure*
    - *pressurepressure*
    - *PRESSURE*
    - *pr3ssur3*
    - *etc...*

# Password attacks – Credential stuffing

- A variant of dictionary attacks
- Attacker uses a list of known username/password combinations **from an earlier breach** and tries every entry in the list on another site
- Exploits the fact that many people use the same username and password on several sites

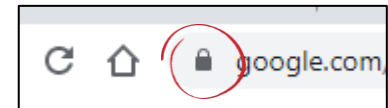
# Social engineering

- Manipulation of people as part of a cyberattack
  - Divulge passwords or sensitive information
  - Performing actions to facilitate a break-in into IT systems
- **Phishing** – send email to trick the receiver into, e.g.:
  - Give up passwords or personal info
  - Download malicious software



# Social engineering – Spoofing

- Attackers are getting increasingly good at spoofing official-looking emails from, e.g., employers, e-commerce sites, government institutions, postal service, etc.
  - Might link to a fake login page – which steals your password
  - Common to use URLs that are similar-looking to legitimate URLs
  - Can use stolen certificates or hacked sites to have TLS encryption (“padlock symbol”)
  - Can even use tricks with *homographs*:
    - For example, the Latin letters “e” and “a” are replaced with the Cyrillic “e” and “a”: **wikipedia.org**



# Social engineering – Spear phishing

- Instead of mass-mailing phishing emails and hoping that someone takes the bait – **use targeted attacks**
  - CEO
  - IT-admin
  - ... or anyone who can (inadvertently) help attackers to get a foothold into system
- Typically entails surveilling target for an extended period of time to learn, e.g.:
  - Role and responsibilities in organization
  - Contacts
  - Interests (personal, professional)
- Send tailor-made phishing email to pique target's interest



# Malware

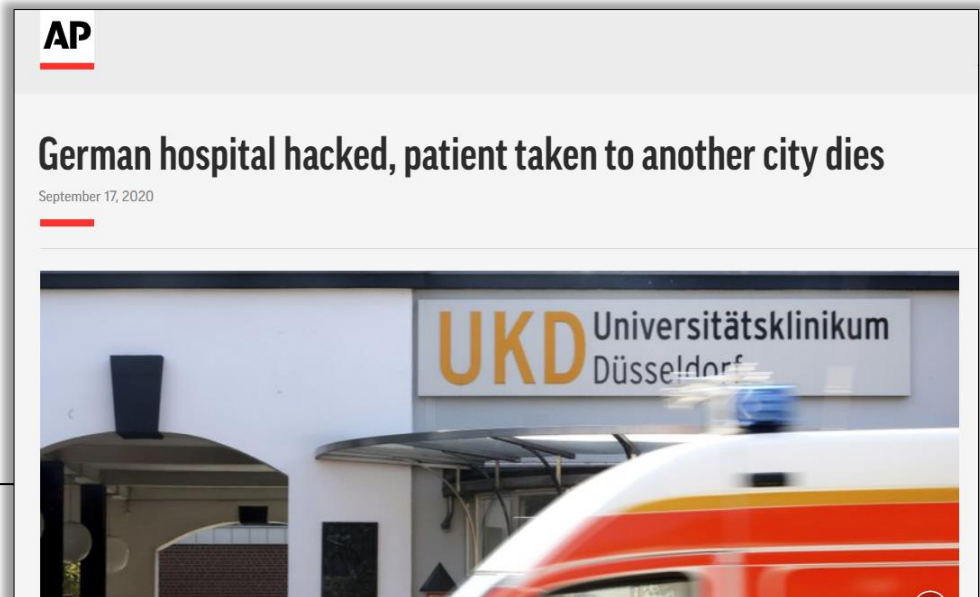
- Software designed with the *intention* of causing some harmful effects.
  - Spyware
  - Botnet clients
  - Ransomware
  - ...
- Most malware today are *trojans* – requires some action from the victim
  - Download “free” pirated software
  - Spoofed emails
    - Open malicious email attachment
    - “You need to install this important software update...”

# Malware

- **Spyware** is designed to steal, e.g., passwords, credit card numbers, etc.
- **Botnet clients** silently turn victim machines into a remotely controlled member of a *botnet*
  - Victim is often unaware of the infection...
  - ...but the attacker can remotely instruct all infected machines to perform denial-of-service attacks against websites
    - Flood website with repeated connection attempts from thousands of hijacked computers
    - Often used for extortion or hacktivism

# Malware – Ransomware

- Encrypt all files on hard drive. Demand ransom to be paid for restoring the system.
- Might also exfiltrate sensitive files – can be used as leverage to persuade victim to pay up
- Some attacks use the “shotgun approach” – send spam emails with, e.g., malicious links
  - Some will fall for it and get infected
  - Can also spread over a network to infect vulnerable machines
  - Sometimes with inadvertent disastrous effects ...



# Malware – Ransomware

- However, **targeted attacks** are becoming increasingly common
  - Carefully planned operations by professional hacker groups
  - Often executed over the course of several months
- Might use spear phishing to gain initial foothold into system
- Infiltrate other systems over an extended period of time – until attackers are ready
  - Cripple entire IT-infrastructure and demand ransom



# Software exploits

- Programs can have bugs (programming mistakes) that allows manipulating their behavior
  - Such bugs are known as *software vulnerabilities*
- By providing a specially-crafted input to a vulnerable program, attackers can sometimes “trick” the program into executing the attacker’s commands
  - For example, download and install malware
- The specific procedure used to trigger a vulnerability is called an *exploit*

# Software exploits

Can be used to spread malware

- Malicious e-mail attachments (PDF, Word, etc.)
  - When opened with a vulnerable document viewer, installs malware
- Malicious web page – enough to *view* the web page with an old, vulnerable version of a web browser
- Can also be used to spread malware over a network (e.g., old version of Windows with file-sharing enabled)

## **This is why most modern software have auto-update functionality!**

- However, not all software can be updated
- For example, medical equipment – cannot modify in any way (including software) without voiding safety certification
  - These things are often PC computers “under the hood”, running an old Windows version...

