Stockholm University

Intro to InfoSec - Authentication

Stefan Axelsson, Nov. 2020

Today – Authentication

Stockholm University

- Chapter 2.1 in Pfleeger et.al. *Security in Computing*, 5th ed.
- Authentication – The art of proving who you are
  - Authentication
  - The three bases of authentication
    - Knowledge, characteristics, possessions
  - Strength of an authentication mechanism

Introduction

Stockholm University

- We’re starting from the beginning
- These are tools that touches on many areas and techniques of security (not just info sec)
- You’ve heard of a security policy
  - What are the parts?
    - Who, what, how
      - Who (subject) can access
      - What (object)
      - How (method)
- Here we’ll focus on the ”who” – Subjects

Today – Authentication

Stockholm University

- The first step if determining ”who”
  - You’ll of course have to have mechanism to do that – If you have no way of limiting access, then it doesn’t matter
    - More about that later
- So first:
  - Identification
  - Authentication
  - (Authorization)

Identification

- **Identification** – Asserting who you are
  - Doesn’t have to be a person
    - Could be a ”computer” or ”email adress” or something similar
  - Often we don’t think about it
    - When you send an email you’ll include a return email adress saying who it’s from
    - Also telephone number, bank account number, Swedish ID number (*personnummer*)
    - So we often conflate it with authentication but **it’s distinct**

Identification

- **Identification**
  - But note, this doesn't **prove** who you are
    - Person to person it's implicit – We recognise each other, but remotely it's difficult
  - Identities are most often public
  - They're not secure – Many people could claim to be you by using your identifiers
    - Many security problems stem from accepting identification as authentic

Authentication

- Authentication – Should be private
  - This is proving who you are
  - There are in general three ways
    - Something you know – Shared secret
    - Something you are – Biometrics
      - Something you intrinsically are
      - The way you do something
    - Something you have – Token
  - (OK so four ways then…)

Authentication

- Authentication
  - Something you know – Shared secret
    - Passwords, PIN, passphrase, a secret handshake, mother's maiden name
  - Something you are – Biometrics
    - Something you intrinsically are
      - Fingerprint, iris pattern, look of **face**
    - The way you do something
      - Pattern of your **voice**, walk, sign your signature,
  - Something you have – Token
    - Identity badge/card, physical key, uniform

Authentication

- Authentication – Note that
  - Face – In person and
  - Voice – On the phone
- Are the main two ways we identify people known to us – and have for a long time
- And we’re quite happy with them, they rarely fail even though one is probably better than the other
  - It’s more difficult to fool someone with a mask in person, than on the phone

Authentication failures

Stockholm University

- When we can’t do face-to-face failures abound
- We’ll look in detail at **shared secrets – Something you know**
- A problem here is that while passwords can be secure what do you do when it’s been forgotten?
  - You ask ”security questions”
    - Supposed to be easy to remember facts about the person
      - Mother’s maiden name, favourite colour, father’s middle name

Authentication failures

Stockholm University

- **Security questions**
- Problem with these are that they’re not necessarily secret
- So George Bronk (and others) trawled facebook for email addresses and also clues to their security questions
- Then contacted email providers and pretended to be user that had lost password
  - Was often successful in guessing answers to security questions
- Then checked sent email for explicit/embarrasing photographs

Authentication failures

Stockholm University

- How do passwords work?
  - User supply identification and passwords
  - Given PW is compared for PW on file for given identification
- So as we saw: Autenticators need to be secret
- Other problems
  - Use – Supplying a password for each access to an object is inconvenenient(!)
  - Disclosure – If user discloses PW then game is up
  - Revocation – Someone must change PW
    - Causing same problem as disclosure

Authentication failures

- Loss – If user forgets/discloses PW then new one needs to be assigned
  - Need to ensure that this isn't same as before

Passwords

How secure are passwords?

- They are often limited in the number of bits they provide
- And, worse, users don't even use all the available bits – They chose passwords from a limited set, and passwords that are easy to guess
- Security of passwords rely on attacker not being able to brute force or guess passwords
  - Brute force – Try all possible combinations

Passwords – Attacks

Stockholm University

- Steps to try:
  - No password
  - The same as User ID
  - is or derived from the user's name
  - On a common word list (e.g. password, secret, private) plus common names or patterns (e.g. qwerty, aaaaa, 123456)
  - Contained in short college dictionary
  - Contained in complete English word list
  - Contained in common non-English-language dictionaries

Passwords – Attacks

Stockholm University

- Steps to try cont.
  - Contained in short college dictionary with capitalizations (PaSsWorD) or substitutions (digit 0 for letter O a.s.o)
  - Contained in complete English dictionary with capitalizations or substitutions
  - Same but common non-English dictionaries
  - Brute force trying all alphabetic characters
  - Brute force trying all possible combinations from the full character set

Passwords – Attacks

- Note that the last step will of course (eventually) succeed – But it's so costly that it's supposed to be impossible in practice
- But the other approaches are often successfull
  - There is SW – Password crackers – That help automate this process
    - They often rely on being able to make an infinite number of tries (more later)
    - These come with dictionaries including sci-fi character names, mythological names, Chinese words etc.
    - They also make "obvious" substitutions
      - 0→O, 1→l etc.

Passwords – Attacks

- Password crackers also typically include
  - Passwords based on user – I.e. user name, full name, etc.
  - Other SW do e.g. web crawl to find names of relatives, areas of special interests etc. and seed their PW lists based on these
  - At NSA: Username Kirk ”And then type your password, ’Captain’.”
    - ”How do you know my password???”

Passwords – Attacks

- People are often crap at choosing passwords:
  - Imperva analyzed 34 million Facebook PW 2009
    - 30% fewer than 7 chars
    - 50% used names, slang words, dictionary words and trivial passwords
      - Consecutive digits, adjacent chars on keyboard etc.
        - 12345, 123456, ”password”, ”iloveyou”
  - Realise that there are a lot fewer words than possible passwords!

Passwords – How to store them?

Stockholm University

- Just list with all passwords? No! Horrible idea!
  - Encrypt them

TABLE 2-2 Sample Password Table

Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

TABLE 2-3 Sample Password Table with Concealed Password Values

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Passwords – How to store them?

Stockholm University

- But does encryption in itself work?
  - No, salt them as well – To stop dictionary attack

TABLE 2-4 Sample Rainbow Table for Common Passwords

Original Password	Encrypted Password
asdfg	0x023c94fc
p@55w0rd	0x04ff38d9
aaaaaa	0x13b9c32f
password	0x2129f30d
qwerty	0x471aa2d2
12345678	0x4f2c4dd8
123456	0x5903c34d
aaaaa	0x8384a8c8
	etc.

TABLE 2-5 Sample Password Table with Personalized Concealed Password Values

Identity	ID+password (not stored in table)	Stored Authentication Value
Jane	Jan+qwerty	0x1d46e346
Pat	Pat+aaaaaa	0x2d5d3e44
Phillip	Phi+oct31witch	0xc23c04d8
Roz	Roz+aaaaaa	0xe30f4d27
Herman	Her+guessme	0x8127f48d
Claire	Cla+aq3wm$oto!4	0x5209d942

Passwords – How to store them?

Stockholm University

- So long passwords (passphrase), use ”all” characters, different passwords for all uses
- Don’t tell anyone – Even if they say they’re support
  - Called ”social engineering”
- Book says not to write down
  - True if that means ”post IT on screen”
  - False if it means PW safe software
    - Recommendation is to use said
      - E.g. any of the KeePass variants

Passwords – Usability

- This is a problem
  - One would be OK
    - Hundreds not so much
  - Also all or nothing – You must remember it perfectly
    - That’s now how human memory works
  - To be good it has to have no structure
    - Be ”random”
      - This is even harder to remember

Other things you know

- Other things have been proposed
  - Mobile phone pattern screen unlock
  - Various patterns using images (image selection)
- Not well researched and haven't become very popular (with one or two exceptions)
  - Security can also be lacking
    - This is esp. True with "security questions"
      - Don't use them – Or mangle them (i.e. add four numbers a.s.o)

Stockholm University

Biometrics

Stefan Axelsson, Nov. 2020

Biometrics

Stockholm University

- Biological properties that you can measure
  - Hence Bio-Metrics
- Non exhaustive list of things that can be measured and are used:
  - Fingerprint, hand geometry, retina and iris (eye), voice,
  - handwriting, signature, hand motion, typing characteristics, blood vessels in the finger/hand, face, facial features (nose shape/eye spacing)

Biometrics

- Examples Hand geometry, and hand vein reader

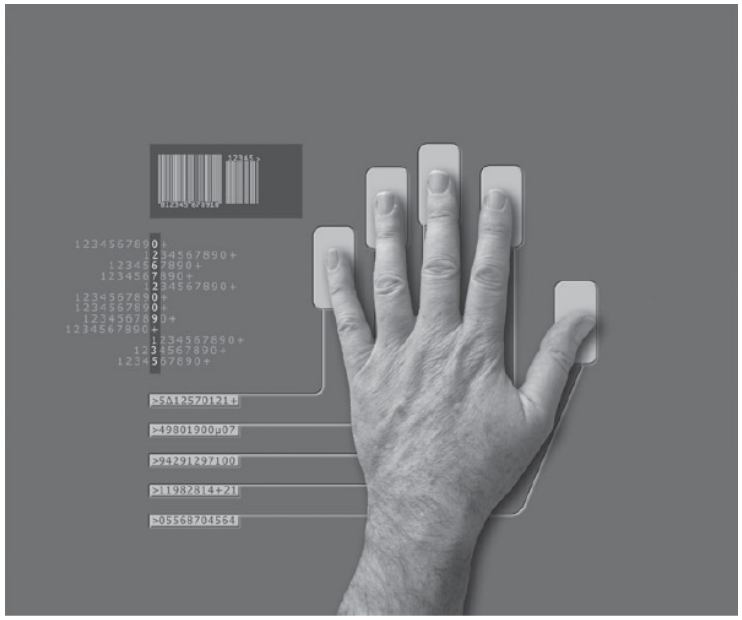

FIGURE 2-2 Hand Geometry Reader (Graeme Dawes/Shutterstock)

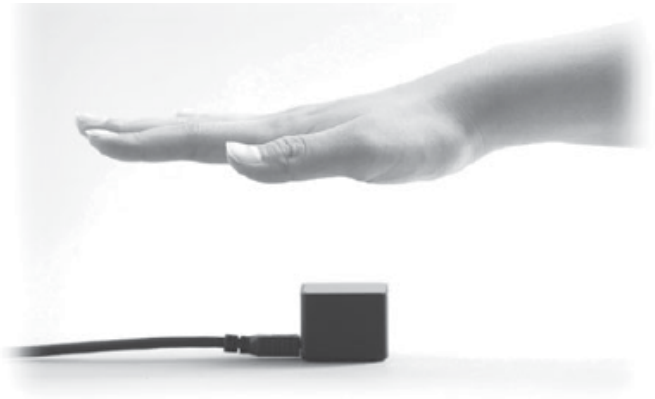

FIGURE 2-3 Hand Vein Reader (Permission for image provided courtesy of Fujitsu Frontech)

Biometrics – Problems

- Relatively new – Some find it intrusive
  - Laser beam in the eye someone?
- Costly – Some devices (fingerprint readers) are cheaper now
  - But then not as good? And how do you know?
- Single point of failure
  - I can get a new password, but not a new eye, or finger
    - Also not always secret – Face recognition?
- They sample and hence no exact match
  - What about damaged finger, or cold voice

Biometrics – Problems

Stockholm University

- Failure to enroll – Failure to acquire
  - Not in book (by these names) – Not everybody have the feature, at least not all the time
    - Injury, temperature, humidity etc.
- Speed can limit accuracy
  - Many samples can increase accuracy, but takes time we may not have
- There are forgeries
  - Not the person – Its a signal from a sensor
    - If you can fool sensor you can fool system
      - Fake finger, picture of face, etc.
        - Brazilian doctor with 16 fingers...

Binary decision theory

- False positive, false negative etc.

Binary test	Is person	Is not person
Test postitive (Match)	True positive	False positive
Test negative (No match)	False negative	True negative

- Positive/Negative is the test
- False/True is the reality
- Hence, False Positive = Test says match, but that's not true, i.e. false
  - Also specificity, sensitivity, accuracy etc. Read book

Binary decision theory

- ROC – Curve
  - Often we can adjust the sensitivity of a test
  - More sensitive, then more (true) hits, but also more false hits (nervous system)
  - Less sensitive, fewer (true) hits, but also less false hits (phlegmatic system)
- If you plot TP rate vs. FP-rate

  you get a ROC curve
  - Receiver Operating Characteristics

SIDEBAR 2-6 *Continued*

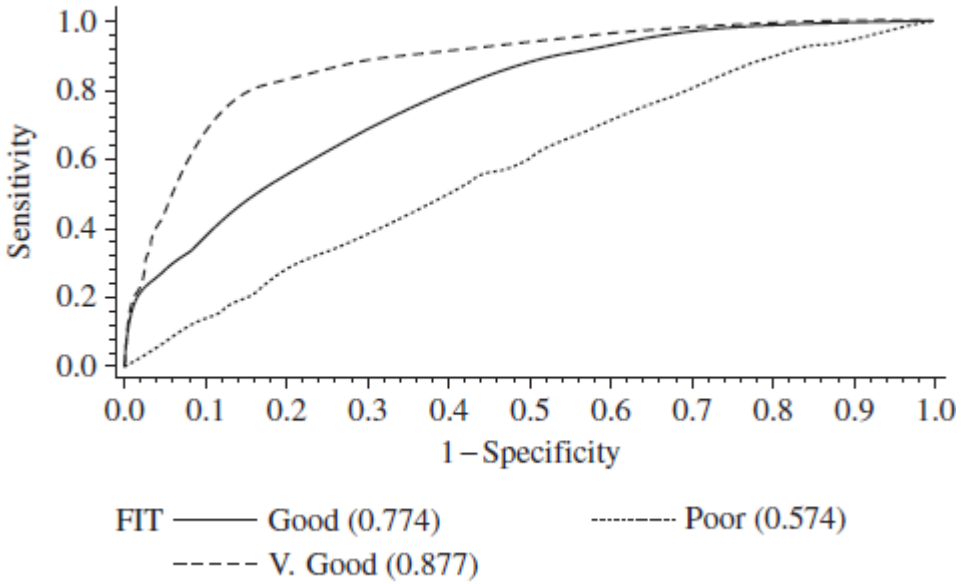

FIGURE 2-4 ROC Curves

Biometrics

- Inexact match leads to many problems
  - Too exact – it won't work
  - Too loose – too many false matches
    - Note iPhone fingerprint reader that requires PIN auth regularly
    - And higher risk of forgeries
- Also these systems are often not as good as people think
  - DNA match is good if
    - DNA is not degraded
    - We're not doing drag net searches
      - 1/11 million only if one match
        - With 6 million possibilities then ½...

Biometrics

- Same with fingerprints
  - Madrid bombing had false match
    - Brandon Mayfield, U.S. lawyer in Oregon arrested by FBI – They called it 100%, but was obviously not

Biometrics

Stockholm University

- So, have advantages
  - Can’t forget a biometric
- But also problems
  - Can be forged as they’re often not secret and matches have to be inexact
  - Can’t be changed if they do leak
  - Not everyone have them, at least not all the time, and they can change over time
    - Hair colour in passport… (I used to be blond…)
  - There are statistical problems when you try a match against a large database of possible matches
    - Identification+authentication or just identification

Stockholm University

Tokens

Stefan Axelsson, Nov. 2020

Tokens – Something you have

Stockholm University

- Now we come to the last part – Something you have
- This means a physical object that demonstrates that you are who you say you are
  - A (physical) key
    - Conflated with autorization – Possession of the key means you're allowed access
      - Authentication is an after thought
    - Drivers licence
      - Also authorizes when you drive
    - Access badge/card
    - Uniform – Police, customs, firefighter etc.
    - Passport – Perhaps the quintessential authenticator

Tokens – Active/Passive

Stockholm University

- Tokens come in two forms
  - Passive
    - Doesn't change – Driver's license, photo, key
  - Active
    - Interacts with its surroundings and changes
      - Subway card with balance on mag-stripe
- This leads to Static/Dynamic distinction
  - Static – Values remains fixed
    - Keys, ID card, credit card etc.
      - Most useful for on-site ID
        - It's easy to check e.g. photo etc. when you're right in front of guard

Tokens – Static/Dynamic

Stockholm University

- Dynamic – These change, in reply to some challenge typically
  - Needed for remote authentication
    - Guard can't easily verify your face is same as ID remotely
      - Image could be faked (mask?) etc.
- Why do we need them?
  - Static tokens vulnerable to skimming
    - Attacker copies information on token and then reuses it
      - C.f. credit card number from mag-stripe at ATM – then forge card and use elsewhere

Tokens – Dynamic

- Dynamic tokens change, so that isn't possible
  - Either challenge – response
    - You'll have to wait until after crypto
  - Or just change
    - RSA – Secure ID token changes once a minute and generates a new "unpredictable" six digit code – Attacker has one minute to skim and use

Wrapping up

- Federated ID management/Single Sign On
  - But we drown in autentication ourselves all the time
  - Wouldn't it be nice if we could do it once and for all?
  - Federated ID/Single Sign On (Usage not that strict)

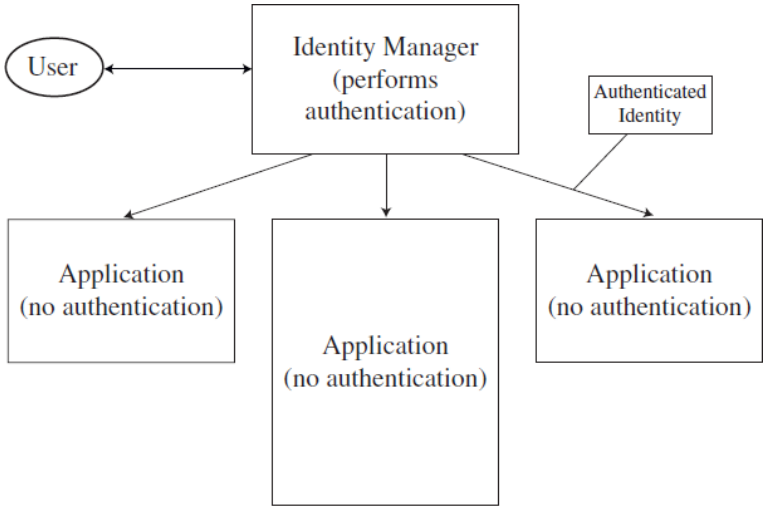

FIGURE 2-7 Federated Identity Manager

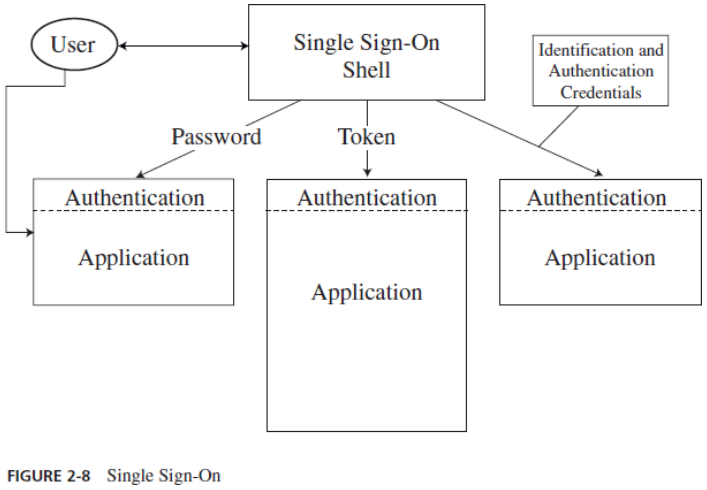

FIGURE 2-8 Single Sign-On

Wrapping up – Multi factor

Stockholm University

- What if it doesn't work
  - You lose your token? Overheard password? Faked image?
  - Multifactor Authentication
    - Use two (most popular) or more ***different kinds*** of authentication
      - I.e. not two passwords, but e.g. PIN ***and*** (chip based)Card (aka "PIN and Chip")
    - Old idea – Passports and Driver's licence contain you signature and picture
      - People can check signature and photo (two kinds of biometric) and that you have card (token)

Summary

- Identification, authentication, (authorization)
- Something you
  - Know – Shared secret
  - Are – Biometric
  - Do – Biometric
  - Have – Token based
- Multi factor – Use two or more different kinds
- Think about attacks and how to thwart them