Lecture 1
zondag 8 september 2022 23:37

access and

XACML

privacy
- definition
- threats

Objective; dependent on culture, context, stakeholders
e.g. right to be let alone
right to decide which information concerning you should be accessible to others and control
freedom from unreasonable constraints on the construction of one's own identity

privacy as confidentiality

location - dataminion
RFID
social networks

all concern personal information, all deal with the confidentiality

What are privacy threats?

misuse of data for secondary usage
misuse of data collection
unauthorized sharing
surveillance
government privacy rights abuse

categories

information collection
information processing
information dissemination
invasion

secondary usage → use of data for different purposes than intended one (e.g. marketing)
aggregation → combining + comparing information → paints more detail individual
↳ use for job applications, credit assessment

video surveillance → used for safety, but can locate people

invisible information gathering
profiling
identity theft
discrimination

privacy is becoming more relevant because powerful computers have enabled more significant threats and information is available digitally more often

ways of locating people
IP address
GPS
phone data
MAC address
social media pictures
Bankcard location
Bankcard / credit card

location based services are used for many purposes
but can also cause privacy issues
and harm (sensitive) beliefs (e.g. politically sensitive thoughts)

RFID → many chips that emits signal when scanned to certain reference
↳ traceability
disclosure of intimacy private
discrimination

Social networks can be used for many other purposes

Privacy enhancing technologies:
- VPN
- Tor
- Encryption
- Decentralization
- Authentication
  - Two-factor authentication
- Federated learning
- Access control

Paradigms:
- Privacy as control
  - Assumptions
    - Collection and processing of personal information is useful & necessary
      - Search engines can improve results/algorithms
    - Organizations have an interest in protecting privacy
    - Privacy issues arise when information is misused
  - Threats
    - Database of queries can be breached
      - Information made public
      - Sold for profit
    - Query data can be used for illegitimate purposes/secondary uses
    - Data shared without user consent
    - Data stored longer than needed
  - Goals
    - Provide control over data
      - Informed consent
      - Privacy settings
        - Privacy preference languages
        - Default suites of privacy settings
        - Privacy wizards
        - Enforcement of privacy settings *is done by organization*
    - Provide compliance with data protection regulations
      - Define & enforce security + privacy policy
      - Prevent/detect misuse of personal information
  - Main characteristics
    - Privacy is defined as the ability to specify acceptable data usage through policies
    - Assumes that organizations are trusted to enforce policies
- Privacy as Confidentiality
  - Assumptions
    - Lack of transparency and data protection enforcement
      - Once organization has data, you cannot (practically) verify how the data is used
    - Organizations are not competent/honest, security is expensive
      - Incentive to use data for financial gain
      - Large number of reported privacy breaches (lack of appropriate security practices)
    - Placing trust in organizations makes individual vulnerable
  - Threats
    - Queries are sensitive
    - User information can be linked across different contexts
    - User profiles can be inferred (data aggregation)
    - Queries are hard to anonymize
    - Massive collection of user information is a privacy threat *in itself*
      - Allows discrimination, manipulation, opportunistic abuse
      - Information asymmetries reinforce power asymmetries
  - Goals
    - Minimize information disclosure
    - Create individual autonomous sphere free from intrusion
    - Disclosure of information is prevented by default, or minimal amount of information is disclosed
  - Main characteristics
    - Privacy is defined as properties hard-coded in the technology itself
    - Preventing data disclosure
    - Minimize the need to trust others for handing sensitive data
- Privacy as practice
  - Assumptions
    - Transparency provides users with an understanding of the system
      - Produces awareness
      - Evokes actions
  - Threats
    - User has no means to know
      - Which data is collected
      - For which purpose data is used
      - How data is aggregated
      - Which decisions are made based on models
  - Goals
    - Focus on user awareness
    - Data collection is made transparent
    - Data processing is made transparent
  - Main characteristics
    - Support users in decision-making
    - Potentially uncover malicious behavior by organizations

Purpose-based Access Control
- Regulate access to data
- Privacy-aware Access Control languages
  - Specify which actions can be performed
  - Specify allowed use of data
- Policy enforcement

Problem: no control after disclosure of data (e.g. if user asks to use data for *a*, they may actually use it for *b*)

Purpose Control
- Verify whether data has been used for the intended purpose
- Auditing mechanism

Anonymous credentials
- Based on zero-knowledge
- Prover can prove
  - He holds a credential with certain attributes
  - Any expression on them (e.g. Boolean, simple arithmetic)
    - Age > 18
    - Gender

Tor
- Anonymous communication over a computer network
- Route traffic through overlay network
- Difficult to trace users' internet activities

Steganography & covert communications
- Encryption hides content
- Anonymity/unlinkability: hide identity/relations
- Unobservability: hide existence
- Communications:
  - Hide the fact that there are any communications
  - Embed communication in another piece of communication
  - Covert channels: hide secrets within public information
- Storage
  - Hide the existence of files
  - Allows denial of existence of files

P3P: Platform for Privacy Preferences
- Allow websites to communicate their privacy policies
- Provides a standard XML format to encode privacy policies
- Help users understand privacy policies

Lacks enforcement

Transparency tools
- Give users a better understanding of information flow, state & history
- Examples
  - Google 'dashboard'
  - Facebook (view how others see your profile)