Outline

- Privacy as a security property
  - Hard and Soft Privacy
- Hard privacy primitives
  - Anonymous communications, credentials and e-cash, censorship resistance, steganography
- Soft privacy solutions
  - Privacy policies, audit controls, certification, process
- Specific applications
  - Medical systems, Election systems, transport
- The future of privacy technology
  - Challenges, economics, legislation
Definitions of Privacy

- **What is Privacy?**
  - "The right to be left alone"
    - Confidentiality
  - "Informational self-determination"
    - More general: control

- **Socio-legal rules**
  - Data protection principles
    (EU, Canada, Australia, ...)
  - US: Fair information practices
    (HIPPA, California disclosure laws, ...)
Data Protection Principles

- Personal data:
  1. Shall be processed fairly and lawfully
  2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose(s)
  3. Shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed”.
  4. Shall be accurate and, where necessary, kept up to date.
  5. **Processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**
  6. Personal data shall be processed in accordance with the rights of data subjects
  7. Appropriate technical and organisational measures shall be taken **against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
  8. Personal data shall not be transferred to a country or territory outside the European Economic Area,...
Implementation of data protection requirements

- Data protection authorities
  - Make rules, judgments

- Reporting vs no reporting
  - What data is processes

- Data protection officers in data holders
  - In charge with compliance

- Data subject rights
  - Right to access, to know, to correct, to compensation

- General rule: weak enforcement, low penalties
Technology and privacy protection

- Support data protection principles

- Hard privacy: data minimization
  - (data never leaks)
  - Threat model: data holder might be bad.

- Soft privacy: support other properties
  - (security, control, data access, deletion)
  - BUT: data subject has lost control of the data
  - Threat model: third parties, corrupt insider within honest data holder, errors, ...

- Note on threat model: inequality of power.
Privacy Technology and security

- Infrastructure privacy:
  - Telecommunications (GSM)
  - Authentication
  - Payments
  - Transport
- Good for individuals
- But also good for business, government, national security
  - Infrastructure is cheap, robust -> shared
  - All will use it: Military, Gov, Business, Police, ...
  - Weaknesses against privacy will impact them!
- Security and Privacy are not opposed to each other.
Hard Privacy: Communications

- Traditional security for communications:
  - Confidentiality, Integrity of data
  - Non-repudiation

- Privacy properties (Off-the-record):
  - Confidentiality, Integrity (same)
  - Repudiation (opposite)
  - Forward security (compulsion)

- More privacy properties:
  - Anonymity (sender, receiver)
  - covertness
  - censorship resistance (availability)
Off-the-record messaging

- Privacy properties (Off-the-record):
  - Confidentiality, Integrity (same)
    (Authenticated DH Key exchange)

- Forward security (compulsion)
  (Ephemeral keys using DH, delete them at the end)
  (Keep updating the keys: exchange nonces, hash old key with nonces.)

- Repudiation (opposite)
  - Option 1: Use of MACs instead of signatures.
  - Option 2: Use signatures and publish the keys at the end.

- (You can download it for gAIM)
Anonymous communications (I): what?

- Who talks with whom leaks information
  - Intentions and plans
  - Profiling of users

- Several anonymity properties:
  - Mail
    (sender, receiver, full, third party)
  - Web
    (client, server)

- Can authenticate over the anonymous channel.
  - As well as run any other complex security protocol.
Systems for anonymous communications

- Theoretical / Research track:
  - Mix networks (1981)
  - DC-networks (1985)
  - ISDN mixes (1992)
  - Onion Routing (1996)
  - Crowds (1998)

- Real World systems:
  - anon.penet.fi (one-hop, 1988)
  - Remailers: Type 0, Type I, Mixmaster (1994)
  - Anonymizer (90s)

- State of the art:
  - The Onion Router (Tor) (2005)
Attacks against anonymous communications

- Traffic Analysis: against vanilla or hardened systems
- Extract information out of patterns of traffic (no content)

- Attacks on anonymity systems:
  - Traces who is talking with whom,
  - extract profiles

- Families of attacks:
  - Long term black box,
  - tracing streams in the network,
  - cryptography.)

- Young science -- expect a lot of progress over the next few years.
Hard Privacy: Entity and attribute authentication

- (Bart Preneel has given an overview of entity authentication.)
- Many aspects of authentication:
  - Identify principal to use in access control (computer security)
  - Share a key to communicate securely (cryptography)
  - Verify some attributes
- Result: authentication is often the first step of any transaction.
- Problem: privacy invasion -- against data minimization (and the real world).
Attribute Authentication and credentials

- Attribute verifications:
  - Identity documents: the state certifies your name, age, address, ...  
  - Letters of reference: employer certifies your salary for your landlord  
  - Club membership: the club certifies you are a gold member

- Credential: token that allows you to certify an attribute.

- Entities:
  - Issuer (State, Employer, Club)
  - Prover (holder of the certificate)
  - Verifier (anyone!)

- Property: prover proves to the verifier that he holds a credential with certain properties
  - Properties: Privacy and unforgeability
Anonymous credentials

- Cryptographic protocols between <Issues, Prover, Verifier>
  - Based on zero-knowledge
  - Prover can prove that he holds a credential with certain attributes
    or any expression on them (simple arithmetic, boolean)
    (e.g. UGC ladies nights: age > 18 and gender = female)
  - Verifier gains no more information
  - Name of prover is hidden from verifier and issuer

- Two types of unlinkability
  - Single show credentials
    (Shows are linkable - simple & cheap) (Chaum and Brands)
  - Multi-show credentials
    (Shows are not linkable - complex) (Camenisch and Lysyanskaya)

- Security: cryptographic (Hard Privacy)
Hard Privacy: E-cash

- Secure and private payments
  - Cannot forge money or payments
  - with the anonymity of cash
  - Not just cash: cinema tickets

- Adapt anonymous credentials
  - The bank certifies I have one euro
  - Payment: prover shows the credential, verifier accepts it
  - Verifier goes to the bank to deposit the coin

- Security properties:
  - Unforgeability
  - Privacy (for payer)
  - Double spending prevention!

- More twists for efficient issuing
Hard Privacy: Steganography and covert communications

- What do we have so far
  - Encryption: hides data content
  - Anonymity: hides entities
  - Steganography: hides existence...

- Communications:
  - Hide the fact that there is any communications
  - Embed a communication within another
  - Covert channels: hide secrets within public information

- Storage:
  - Hide the existence of files
  - Under coercion can deny there are any files to decrypt
  - Threat models: snapshots of system, network file system
Hard Privacy: Censorship resistance

- How is that privacy technology?
  - Communities, tools, and techniques overlap.
  - Second definition: information self-determination
  - Freedom (and techniques) to conceal information or to communicate

- Censorship resistance in communications:
  - Firewall busting techniques (national firewalls)
  - Economic importance: skype, and NATs.
  - Peer-to-peer networking and file sharing.
    (Combine anon.comms, replicated storage, ...)

- Censorship resistance is the new availability!
  - One of the killer apps of the 00s.
Turning to Soft Privacy

- **Difference with Hard privacy**
  - Sensitive data is divulged (identity, medical condition, preferences, profile)
  - Need to still guarantee some properties (Deletion, appropriate use, subject access)

- **Limits to these technologies:**
  - No direct control of data subject
  - Cannot defend against a malicious data holder / superuser
  - Weaker threat models: errors, carelessness, corrupt insider, ...

- **Guaranteeing strength of mechanisms *would* be expensive**
  - Verify and certify that systems work as claimed
  - "Thankfully" no one asks for such a verification
  - So they are the most popular
Soft Privacy: Privacy policies on the Web

- Early days:
  - you had no idea what happened to your data on the web
  - against data protection (informed consent)
  - Best practice: tell what happens to the data

- Technological support:
  - P3P language
  - Allows to specify the attributes sought
  - Browsers can be configured to inform you, accept or reject

- Future or dead end? Negotiation
  - The client and merchant negotiate about the data to be transferred
  - Enormous complexities
  - Process itself should not leak & not bother user

- Note: no enforcement, only informational
Soft Privacy: Privacy policy languages

- Once the data is being processed what happens?
  - Difficult to guarantee without being able to express it.
  - EPAL: Enterprise Privacy Language (IBM Research)
  - Can specify what happens to the data

- The problem of enforcement
  - Can drive a mandatory access control policy to protect privacy
  - Can protect against dishonest users
  - Cannot protect against dishonest party
  - Obligations: deletion, reporting and auditing

- Poor deployment so far.
Example applications: Medical privacy

- Medical information is sensitive
  - high integrity
  - Yet need for timely access
  - (Privacy only comes last)

- Different approaches
  - Trust assumptions
  - NHS Spine: everyone trusts the NHS
  - BMA model: distribution of trust by keeping records in local doctors
    (Distribution of trust as a security strategy)
Example applications: Secure Electronic Elections

- Cryptographic security instead of chain of custody.
- Security properties
  - Correctness
  - Receipt-freeness (cannot sell votes)
- Stronger security than real-life elections:
  - Public verifiability: ensures that all can check that election was correct
- How?
  - Voter authentication ->
  - casting encrypted ballot ->
  - verified mixing ->
  - opening of ballots
- New companies are popping up
Privacy in Transport and Car-to-car communications

- Old days:
  - Paper tickets in transport
  - Cars do not chat

- Now:
  - Electronic tickets, pre-payed tickets, ...
  - Pay-as-you drive insurance

- Future:
  - Cars exchange information
  - Location based services

- New sensitive item: Location

- Solutions: mix zones. Will it work?
What future for Privacy Technology

- Compliance is a strong driver
  - Data Protection
  - US disclosure legislation

- Soft Privacy is the state of the art
  - Hidden costs of securing the data silos
  - Issue of liability

- Hard Privacy solutions:
  - Active research
  - Poor deployment (cost, crypto-restrictions)
  - Sensitivity to location might be a key application
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Nunc pulvinar est sed velit.
Sed ac nulla dignissim lectus semper laoreet.
Vestibulum rutrum interdum quam.
Nunc ullamcorper hendrerit justo.
Mauris ut ante nec augue posuere lobortis.

Cras facilisis aliquam mauris.

Aenean varius nisi ut urna.

Quisque volutpat dignissim sem.

Curabitur nec dui ut nisi pulvinar hendrerit.

In dapibus justo in elit.

Nulla sit amet felis a tellus vulputate vehicula.