Access Control and Privacy Policies (7)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also homework is there)

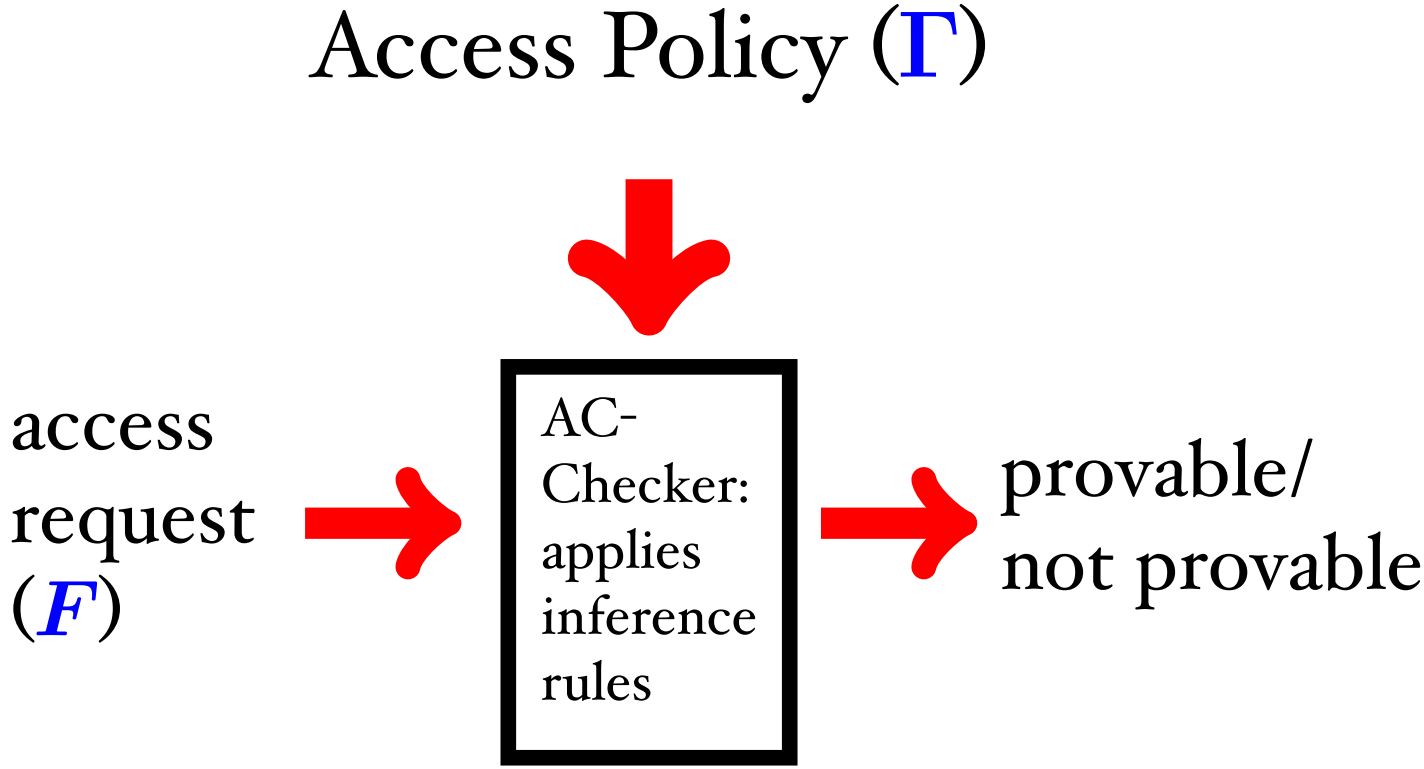
Recall the following scenario:

- If Admin says that file should be deleted, then this file must be deleted.
- Admin trusts Bob to decide whether file should be deleted (delegation).
- Bob wants to delete file.

$$\Gamma = \begin{array}{l} (\text{Admin says del\_file}) \Rightarrow \text{del\_file}, \\ (\text{Admin says } ((\text{Bob says del\_file}) \Rightarrow \text{del\_file})), \\ \text{Bob says del\_file} \end{array}$$

$$\Gamma \vdash \text{del\_file}$$

The Access Control Problem



- P says F means P can send a "signal" F through a wire, or can make a "statement" F

- P says F means P can send a "signal" F through a wire, or can make a "statement" F

- P is entitled to do F

  P controls $F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow F$

$$\frac{\Gamma \vdash P \text{ controls } F \quad \Gamma \vdash P \text{ says } F}{\Gamma \vdash F}$$

Security Levels

- Top secret (TS)
- Secret (S)
- Public (P)

$$slev(P) < slev(S) < slev(TS)$$

Security Levels

- Top secret (TS)
- Secret (S)
- Public (P)

$$slev(P) < slev(S) < slev(TS)$$

- Bob has a clearance for "secret"
- Bob can read documents that are public or sectret, but not top secret

Reading a File

$$\frac{\text{Bob controls Permitted (File, read)} \quad \text{Bob says Permitted (File, read)}}{\text{Permitted (File, read)}}$$

Reading a File

$$\frac{\begin{array}{l}\boldsymbol{slev}(\text{File}) < \boldsymbol{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted (File, read)} \\ \text{Bob says Permitted (File, read)} \\ \boldsymbol{slev}(\text{File}) < \boldsymbol{slev}(\text{Bob})\end{array}}{\text{Permitted (File, read)}}$$

Reading a File

$$\frac{\begin{array}{l} \mathit{slev}(\text{File}) < \mathit{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted (File, read)} \\ \text{Bob says Permitted (File, read)} \\ \mathit{slev}(\text{File}) = \mathit{P} \\ \mathit{slev}(\text{Bob}) = \mathit{S} \\ \mathit{slev}(\mathit{P}) < \mathit{slev}(\mathit{S}) \end{array}}{\text{Permitted (File, read)}}$$

Substitution Rule

$$\frac{\Gamma \vdash \boldsymbol{slev}(\boldsymbol{P}) = \boldsymbol{l}_1 \quad \Gamma \vdash \boldsymbol{slev}(\boldsymbol{Q}) = \boldsymbol{l}_2 \quad \Gamma \vdash \boldsymbol{l}_1 < \boldsymbol{l}_2}{\Gamma \vdash \boldsymbol{slev}(\boldsymbol{P}) < \boldsymbol{slev}(\boldsymbol{Q})}$$

Substitution Rule

$$\frac{\Gamma \vdash \boldsymbol{slev}(\boldsymbol{P}) = \boldsymbol{l}_1 \quad \Gamma \vdash \boldsymbol{slev}(\boldsymbol{Q}) = \boldsymbol{l}_2 \quad \Gamma \vdash \boldsymbol{l}_1 < \boldsymbol{l}_2}{\Gamma \vdash \boldsymbol{slev}(\boldsymbol{P}) < \boldsymbol{slev}(\boldsymbol{Q})}$$

- $\boldsymbol{slev}(\text{Bob}) = \boldsymbol{S}$
- $\boldsymbol{slev}(\text{File}) = \boldsymbol{P}$
- $\boldsymbol{slev}(\boldsymbol{P}) < \boldsymbol{slev}(\boldsymbol{S})$

Reading a File

$$\frac{\begin{array}{l} \boldsymbol{slev}(\text{File}) < \boldsymbol{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted (File, read)} \\ \text{Bob says Permitted (File, read)} \\ \boldsymbol{slev}(\text{File}) = \boldsymbol{P} \\ \boldsymbol{slev}(\text{Bob}) = \boldsymbol{TS} \\ ? \end{array}}{\text{Permitted (File, read)}}$$

Reading a File

$$\frac{\begin{array}{l}\boldsymbol{slev}(\text{File}) < \boldsymbol{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted (File, read)} \\ \text{Bob says Permitted (File, read)} \\ \boldsymbol{slev}(\text{File}) = \boldsymbol{P} \\ \boldsymbol{slev}(\text{Bob}) = \boldsymbol{TS} \\ \boldsymbol{slev}(\boldsymbol{P}) < \boldsymbol{slev}(\boldsymbol{S}) \\ \boldsymbol{slev}(\boldsymbol{S}) < \boldsymbol{slev}(\boldsymbol{TS})\end{array}}{\text{Permitted (File, read)}}$$

Transitivity Rule

$$\frac{\Gamma \vdash l_1 < l_2 \quad \Gamma \vdash l_2 < l_3}{\Gamma \vdash l_1 < l_3}$$

- $slev(P) < slev(S)$
- $slev(S) < slev(TS)$

  $slev(P) < slev(TS)$

Reading Files

- Access policy for Bob for reading

$$\frac{\begin{array}{l}\forall f.\ \mathit{slev}(f) < \mathit{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted } (f, \text{read}) \\ \text{Bob says Permitted (File, read)} \\ \mathit{slev}(\text{File}) = P \\ \mathit{slev}(\text{Bob}) = TS \\ \mathit{slev}(P) < \mathit{slev}(S) \\ \mathit{slev}(S) < \mathit{slev}(TS)\end{array}}{\text{Permitted (File, read)}}$$

Reading Files

- Access policy for Bob for reading

$$\frac{\begin{array}{l}\forall f.\ \mathit{slev}(f) \leq \mathit{slev}(\text{Bob}) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted } (f, \text{read}) \\ \text{Bob says Permitted (File, read)} \\ \mathit{slev}(\text{File}) = \mathit{TS} \\ \mathit{slev}(\text{Bob}) = \mathit{TS} \\ \mathit{slev}(P) < \mathit{slev}(S) \\ \mathit{slev}(S) < \mathit{slev}(\mathit{TS})\end{array}}{\text{Permitted (File, read)}}$$

Writing Files

- Access policy for Bob for **writing**

$$\frac{\begin{array}{l}\forall f.\ \mathit{slev}(\text{Bob}) \leq \mathit{slev}(f) \Rightarrow \\ \qquad\qquad \text{Bob controls Permitted } (f, \text{write}) \\ \text{Bob says Permitted (File, write)} \\ \mathit{slev}(\text{File}) = \mathit{TS} \\ \mathit{slev}(\text{Bob}) = \mathit{S} \\ \mathit{slev}(\mathit{P}) < \mathit{slev}(\mathit{S}) \\ \mathit{slev}(\mathit{S}) < \mathit{slev}(\mathit{TS})\end{array}}{\text{Permitted (File, write)}}$$

Encrypted Messages

- Alice sends a message m

Alice says m

Encrypted Messages

- Alice sends a message m

  Alice says m

- Alice sends an encrypted message m (with key K)

  Alice says $\{m\}_K$

Encrypted Messages

- Alice sends a message m

$$\text{Alice says } m$$

- Alice sends an encrypted message m (with key K)

$$\text{Alice says } \{m\}_K$$

- Decryption of Alice's message

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_K \quad \Gamma \vdash \text{Alice says } K}{\Gamma \vdash \text{Alice says } m}$$

Encryption

- Encryption of a message

$$\frac{\Gamma \vdash \text{Alice says } m \quad \Gamma \vdash \text{Alice says } K}{\Gamma \vdash \text{Alice says } \{m\}_K}$$

Trusted Third Party

Simple protocol for establishing a secure connection via a mutually trusted 3rd party (server):

Message 1 $A \rightarrow S : A, B$
Message 2 $S \rightarrow A : \{K_{AB}\}_{K_{AS}}$ and $\{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
Message 3 $A \rightarrow B : \{K_{AB}\}_{K_{BS}}$
Message 4 $A \rightarrow B : \{m\}_{K_{AB}}$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

$$P \text{ sends } Q : F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow (Q \text{ says } F)$$

Trusted Third Party

$$
\begin{aligned}
&A \text{ sends } S : \text{Connect}(A, B)\\
&S \text{ says } (\text{Connect}(A, B) \Rightarrow\\
&\qquad\qquad \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}})\\
&S \text{ sends } A : \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}\\
&A \text{ sends } B : \{K_{AB}\}_{K_{BS}}\\
&A \text{ sends } B : \{m\}_{K_{AB}}
\end{aligned}
$$

Trusted Third Party

A sends S : Connect(A, B)
S says (Connect$(A, B) \Rightarrow$
$\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$)
S sends A : $\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
A sends B : $\{K_{AB}\}_{K_{BS}}$
A sends B : $\{m\}_{K_{AB}}$

$\Gamma \vdash B$ says m?

Public/Private Keys

- Bob has a private and public key: K^{pub}_{Bob}, K^{priv}_{Bob}

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K^{pub}_{Bob}} \quad \Gamma \vdash K^{priv}_{Bob}}{\Gamma \vdash \text{Alice says } m}$$

Public/Private Keys

- Bob has a private and public key: K^{pub}_{Bob}, K^{priv}_{Bob}

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K^{pub}_{Bob}} \quad \Gamma \vdash K^{priv}_{Bob}}{\Gamma \vdash \text{Alice says } m}$$

- this is **not** a derived rule!

Sending Rule

$$\frac{\Gamma \vdash P \textit{ says } F \quad \Gamma \vdash P \textit{ sends } Q : F}{\Gamma \vdash Q \textit{ says } F}$$

Sending Rule

$$\frac{\Gamma \vdash P \textit{ says } F \quad \Gamma \vdash P \textit{ sends } Q : F}{\Gamma \vdash Q \textit{ says } F}$$

$$P \text{ sends } Q : F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow (Q \text{ says } F)$$

Trusted Third Party

$$A \text{ sends } S : \mathit{Connect}(A, B)$$
$$S \text{ says } (\mathit{Connect}(A, B) \Rightarrow \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}})$$
$$S \text{ sends } A : \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$$
$$A \text{ sends } B : \{K_{AB}\}_{K_{BS}}$$
$$A \text{ sends } B : \{m\}_{K_{AB}}$$

Trusted Third Party

$$A \text{ sends } S : \mathit{Connect}(A, B)$$
$$S \text{ says } (\mathit{Connect}(A, B) \Rightarrow \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}})$$
$$S \text{ sends } A : \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$$
$$A \text{ sends } B : \{K_{AB}\}_{K_{BS}}$$
$$A \text{ sends } B : \{m\}_{K_{AB}}$$

$\Gamma \vdash B \text{ says } m$?

Challenge-Response Protocol

- an engine E and a transponder T share a key K
- E sends out a nonce N (random number) to T
- T responds with $\{N\}_K$
- if E receives $\{N\}_K$ from T, it starts engine

Challenge-Response Protocol

$$E \text{ says } N \qquad \text{(start)}$$

$$E \text{ sends } T : N \qquad \text{(challenge)}$$

$$(T \text{ says } N) \Rightarrow (T \text{ sends } E : \{N\}_K \wedge T \text{ sends } E : \mathrm{Id}(T)) \qquad \text{(response)}$$

$$T \text{ says } K \qquad \text{(key)}$$

$$T \text{ says } \mathrm{Id}(T) \qquad \text{(identity)}$$

$$(E \text{ says } \{N\}_K \wedge E \text{ says } \mathrm{Id}(T)) \Rightarrow \mathrm{start\_engine}(T) \qquad \text{(engine)}$$

$$\Gamma \vdash \mathrm{start\_engine}(T)?$$

Exchange of a Fresh Key

A and B share a ("super-secret") key K_{AB} and want to share another key

- assumption K_{AB} is only known to A and B

- A sends B : $A, \{N_A\}_{K_{AB}}$
- B sends A : $\{N_A + 1, N_B\}_{K_{AB}}$
- A sends B : $\{N_B + 1\}_{K_{AB}}$
- B sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$

Assume K_{AB}^{new} is compromised by I

Exchange of a Fresh Key

A and B share a ("super-secret") key K_{AB} and want to share another key

- assumption K_{AB} is only known to A and B

- A sends B : $A, \{N_A\}_{K_{AB}}$
- B sends A : $\{N_A + 1, N_B\}_{K_{AB}}$
- A sends B : $\{N_B + 1\}_{K_{AB}}$
- B sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$
- A sends B : $\{msg\}_{K_{AB}^{new}}$

Assume K_{AB}^{new} is compromised by I

The Attack

An intruder I convinces A to accept the compromised key K_{AB}^{new}

- A sends B : $A, \{N_A\}_{K_{AB}}$
- B sends A : $\{N_A + 1, N_B\}_{K_{AB}}$
- A sends B : $\{N_B + 1\}_{K_{AB}}$
- B sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$ recorded by I

The Attack

An intruder I convinces A to accept the compromised key K_{AB}^{new}

- A sends B : $A, \{N_A\}_{K_{AB}}$
- B sends A : $\{N_A + 1, N_B\}_{K_{AB}}$
- A sends B : $\{N_B + 1\}_{K_{AB}}$
- B sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$ recorded by I
- A sends B : $A, \{M_A\}_{K_{AB}}$
- B sends A : $\{M_A + 1, M_B\}_{K_{AB}}$
- A sends B : $\{M_B + 1\}_{K_{AB}}$
- B sends I : $\{K_{AB}^{newer}, N_B^{newer}\}_{K_{AB}}$ intercepted by I
- I sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$

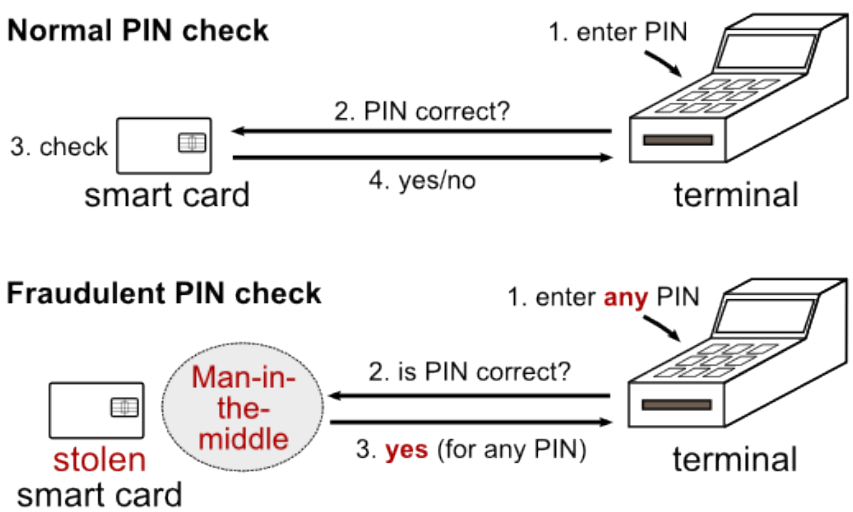
The Attack

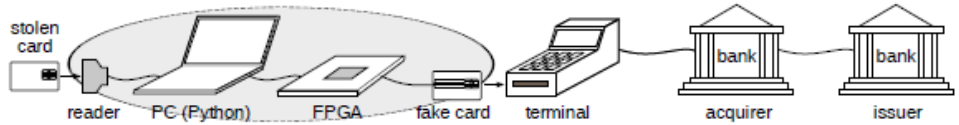
An intruder I convinces A to accept the compromised key K_{AB}^{new}

- A sends B : $A, \{N_A\}_{K_{AB}}$
- B sends A : $\{N_A + 1, N_B\}_{K_{AB}}$
- A sends B : $\{N_B + 1\}_{K_{AB}}$
- B sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$ recorded by I
- A sends B : $A, \{M_A\}_{K_{AB}}$
- B sends A : $\{M_A + 1, M_B\}_{K_{AB}}$
- A sends B : $\{M_B + 1\}_{K_{AB}}$
- B sends I : $\{K_{AB}^{newer}, N_B^{newer}\}_{K_{AB}}$ intercepted by I
- I sends A : $\{K_{AB}^{new}, N_B^{new}\}_{K_{AB}}$
- A sends B : $\{msg\}_{K_{AB}^{new}}$ I can read it also

A Man-in-the-middle attack in real life:

- the card only says yes or no to the terminal if the PIN is correct
- trick the card in thinking transaction is verified by signature
- trick the terminal in thinking the transaction was verified by PIN





Problems with EMV

- it is a wrapper for many protocols
- specification by consensus (resulted unmanageable complexity)
- its specification is 700 pages in English plus 2000+ pages for testing, additionally some further parts are secret
- other attacks have been found
- one solution might be to require always online verification of the PIN with the bank

Problems with WEP (Wifi)

- a standard ratified in 1999
- the protocol was designed by a committee not including cryptographers
- it used the RC4 encryption algorithm which is a stream cipher requiring a unique nonce
- WEP did not allocate enough bits for the nonce
- for authenticating packets it used CRC checksum which can be easily broken
- the network password was used to directly encrypt packages (instead of a key negotiation protocol)
- encryption was turned off by default

Protocols are Difficult

- even the systems designed by experts regularly fail
- try to make everything explicit (you need to authenticate all data you might rely on)
- the one who can fix a system should also be liable for the losses
- cryptography is often not **the** answer

logic is one way protocols are studied in academia (you can use computers to search for attacks)

Public-Key Infrastructure

- the idea is to have a certificate authority (CA)
- you go to the CA to identify yourself
- CA: "I, the CA, have verified that public key P_{Bob}^{pub} belongs to Bob"

- CA must be trusted by everybody
- What happens if CA issues a false certificate? Who pays in case of loss? (VeriSign explicitly limits liability to $100.)

Privacy, Anonymity et al

Some terminology:

- secrecy is the mechanism used to limit the number of principals with access to information (eg, cryptography or access controls)
- confidentiality is the obligation to protect the secrets of other people or organizations (secrecy for the benefit of an organisation)
- anonymity is the ability to leave no evidence of an activity (eg, sharing a secret)
- privacy is the ability or right to protect your personal secrets (secrecy for the benefit of an individual)

Privacy vs Anonymity

- everybody agrees that anonymity has its uses (e.g., voting, whistleblowers, peer-review)

Privacy vs Anonymity

- everybody agrees that anonymity has its uses (e.g., voting, whistleblowers, peer-review)

But privacy?

"You have zero privacy anyway. Get over it."
Scott Mcnealy (CEO of Sun)

If you have nothing to hide, you have nothing to fear.

Privacy

private data can be often used against me

- if my location data becomes public, thieves will switch off their phones and help themselves in my home
- if supermarkets can build a profile of what I buy, they can use it to their advantage (banks - mortgages)
- my employer might not like my opinions

Privacy

private data can be often used against me

- if my location data becomes public, thieves will switch off their phones and help themselves in my home
- if supermarkets can build a profile of what I buy, they can use it to their advantage (banks - mortgages)
- my employer might not like my opinions

- one the other hand, Freedom-of-Information Act
- medical data should be private, but medical research needs data

Privacy Problems

- Apple takes note of every dictation (send over the Internet to Apple)
- markets often only work, if data is restricted (to build trust)
- Social network can reveal data about you
- have you tried the collusion extension for FireFox?
- I do use Dropbox and store cards

- next week: anonymising data

Gattaca (1997)

Privacy

- we do want that government data is made public (free maps for example)
- we do not want that medical data becomes public (similarly tax data, school records, job offers)

- personal information can potentially lead to fraud (identity theft)

Privacy

- we do want that government data is made public (free maps for example)
- we do not want that medical data becomes public (similarly tax data, school records, job offers)

- personal information can potentially lead to fraud (identity theft)

"The reality":

- London Health Programmes lost in June last year unencrypted details of more than 8 million people (no names, but postcodes and details such as gender, age and ethnic origin)

Privacy

- we do want that government data is made public (free maps for example)
- we do not want that medical data becomes public (similarly tax data, school records, job offers)

- personal information can potentially lead to fraud (identity theft)

"The reality":

- also in June last year, Sony got hacked: over 1M users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts.

Privacy and Big Data

Selected sources of "Big Data":

- Facebook
  - 40+ Billion photos (100 PB)
  - 6 Billion messages daily (5 - 10 TB)
  - 900 Million users
- Common Crawl
  - covers 3.8 Billion webpages (2012 dataset)
  - 50 TB of data
- Google
  - 20 PB daily (2008)
- Twitter
  - 7 Million users in the UK
  - a company called Datasift is allowed to mine all tweets since 2010
  - they charge 10k per month for other companies to target advertisement

Privacy and Big Data

Selected sources of "Big Data":

- Facebook
  - 40+ Billion photos (100 PB)
  - 6 Billion messages daily (5 - 10 TB)
  - 900 Million users
- Common Crawl
  - covers 3.8 Billion webpages (2012 dataset)
  - 50 TB of data
- Google
  - 20 PB daily (2008)
- Twitter
  - 7 Million users in the UK
  - a company called Datasift is allowed to mine all tweets since 2010
  - they charge 10k per month for other companies to target advertisement

Cookies...

"We have published a new cookie policy. It explains what cookies are and how we use them on our site. To learn more about cookies and their benefits, please view our cookie policy.

If you'd like to disable cookies on this device, please view our information pages on 'How to manage cookies'. Please be aware that parts of the site will not function correctly if you disable cookies.

By closing this message, you consent to our use of cookies on this device in accordance with our cookie policy unless you have disabled them."

Scare Tactics

The actual policy reads:

"As we explain in our Cookie Policy, cookies help you to get the most out of our websites.

If you do disable our cookies you may find that certain sections of our website do not work. For example, you may have difficulties logging in or viewing articles."

Netflix Prize

Anonymity is necessary for privacy, but not enough!

- Netflix offered in 2006 (and every year until 2010) a 1 Mio $ prize for improving their movie rating algorithm
- dataset contained 10% of all Netflix users (appr. 500K)
- names were removed, but included numerical ratings as well as times of rating
- some information was perturbed (i.e., slightly modified)

All OK?

Re-identification Attack

Two researchers analysed the data:

- with 8 ratings (2 of them can be wrong) and corresponding dates that can have a margin 14-day error, 98% of the records can be identified
- for 68% only two ratings and dates are sufficient (for movie ratings outside the top 500)

Re-identification Attack

Two researchers analysed the data:

- with 8 ratings (2 of them can be wrong) and corresponding dates that can have a margin 14-day error, 98% of the records can be identified
- for 68% only two ratings and dates are sufficient (for movie ratings outside the top 500)

- they took 50 samples from IMDb (where people can reveal their identity)
- 2 of them uniquely identified entries in the Netflix database (either by movie rating or by dates)

- Birth data, postcode and gender (unique for 87% of the US population)
- Preferences in movies (99% of 500K for 8 ratings)

Therefore best practices / or even law (HIPAA, EU):

- only year dates (age group for 90 years or over),
- no postcodes (sector data is OK, similarly in the US)
  no names, addresses, account numbers, licence plates
- disclosure information needs to be retained for 5 years

How to Safely Disclose Information?

- Is it possible to re-identify data later, if more data is released.

- Not even releasing only aggregate information prevents re-identification attacks. (GWAS was a public database of gene-frequency studies linked to diseases; you only needed partial DNA information in order to identify whether an individual was part of the study — DB closed in 2008)

Differential Privacy

User

tell me $f(x)$ $\Rightarrow$

$\Leftarrow f(x) + \text{noise}$

Database

$x_1, \ldots, x_n$

- $f(x)$ can be released, if f is insensitive to individual entries $x_1, \ldots, x_n$
- Intuition: whatever is learned from the dataset would be learned regardless of whether x_i participates

Differential Privacy

User $\quad$ tell me $f(x) \Rightarrow$ $\quad$ Database
$\Leftarrow f(x) + \text{noise}$ $\quad$ $x_1, \ldots, x_n$

- $f(x)$ can be released, if f is insensitive to individual entries $x_1, \ldots, x_n$
- Intuition: whatever is learned from the dataset would be learned regardless of whether x_i participates

- Noised needed in order to prevent queries:
  Christian's salary =
  $$\sum \text{all staff} - \sum \text{all staff} \setminus \text{Christian}$$

Adding Noise

Adding noise is not as trivial as one would wish:

- If I ask how many of three have seen the Gangnam video and get a result as follows

Alice	yes
Bob	no
Charlie	yes

then I have to add a noise of 1. So answers would be in the range of 1 to 3

- But if I ask five questions for all the dataset (has seen Gangnam video, is male, below 30, ...), then one individual can change the dataset by 5

Take Home Point

According to Ross Anderson:

- Privacy in a big hospital is just about doable.
- How do you enforce privacy in something as big as Google or complex as Facebook? No body knows.

Similarly, big databases imposed by government