Scientist's perspective on security and privacy

Andris Ambainis
University of Latvia

Software engineering is about ensuring that certain things happen (“John can read this file”), security engineering is about ensuring that they don’t (“Chinese government cannot read this file”).

Ross J. Anderson, Cambridge University

Challenges

- Data can be:
  - Stored in a cloud;
  - Gathered and analyzed by someone else;
  - Released to public as open data;
- Technology useful for both protecting the privacy and attacking it.

Cloud computing

- Data are increasingly stored on remote computers (“cloud”), possibly belonging to another party.

Do we trust the cloud?

Cloud computing

- Data can be encrypted, making it unintelligible to anyone, except for us.

IBM Research, 2008: Method for computing on encrypted data – without decrypting it

nature International weekly journal of science

Home | News & Comment | Research | Careers & Jobs | Current Issue | Archive | Audio & Video | F

Archive > Volume 519 > Issue 7544 > News > Article

NATURE | NEWS

Extreme cryptography paves way to personalized medicine

Encrypted analysis of data in the cloud would allow secure access to sensitive information.

Erika Check Hayden

23 March 2015

Experiment with analyzing genetic data of 400 people – without decrypting it

Data analysis

- Increasing volumes of personal data is being gathered.
- McKinsey, 2011: Retailers can increase their margins by 60% by exploiting data analytics.

What do we want them to know about us?

Open data

- Certain data should be freely available for use and re-use.
- Having more data openly available will help us discover new and innovative solutions;

Open data vs. privacy

Netflix Prize (2006-2009)

- Open competition to improve movie recommendation system.
- Actual customer data with names/identifying information removed (480 thousand users).
- Very successful, more than 5000 teams.
- University of Texas: several customers identified by name by matching their film rankings with data on the Internet.

Differential privacy

- Field of intense academic interest.
- Established by researchers at Microsoft Research, 2006.
- Goal: methods for releasing statistical information so that ability to learn data of every individual is minimized.

Technology can be useful for both attacking personal data and protecting them