ibbt
connect.innovate.create

ECRYPT II

http://www.ecrypt.eu.org

Privacy Enhanced Communications

Claudia Diaz
COSIC, KU Leuven, Belgium

claudia.diaz@esat.kuleuven.be
http://homes.esat.kuleuven.be/~cdiaz

Data protection: valuable but

- personal data
  - is there truly anonymous data?
  - no need to identify for privacy-invasive practices
  - inferences about others (e.g., gaydar)
- distinction between data controller and data processor
  - complex reality e.g., in a social network
  - or even just visiting a website
- informed consent
  - are there realistic alternatives for the services?
  - do users understand inferences? (entropy of location -> relationship status)
  - backdoor?
- systems should be designed to minimize privacy risks by limiting information leakages (*privacy by design?*)

Communication Privacy

- Privacy is not only about information explicitly provided
  - Gives vs. give-offs: e.g., what you say vs. your body language
- Traffic data
  - Who communicates with whom, when, from where, for how long, how frequently, what is accessed, …
  - Machine-readable + low volume: very easy to process
- Traffic analysis: techniques to analyze traffic data and extract information from it
  - Inferences: provides information on intentions and activities, status in your social circle, location tracking, etc.

Diffie and Landau

- “Traffic analysis, not cryptanalysis, is the backbone of communications intelligence.”
- “Communication is fundamental to our species; private communication is fundamental to both our national security and our democracy.”

- Need to consider traffic analysis threats
  - Otherwise, the protection afforded by other technologies may be rendered useless (eg, anonymous credentials)
- Broad variety of applications:
  - Email, instant messaging, VoIP
  - Social networking platforms
  - Access to public information (eg, web browsing)
  - Mobile devices (location privacy)
- How can we improve privacy protection in communication systems against traffic analysis threats?

International cooperation

- The critical mass of research into communication privacy is in North America (mainly USA and Canada)
  - University of Illinois Urbana Champaign
  - University of Waterloo
  - University of Minnesota
  - University of Texas Arlington
  - U.S. Naval Research Laboratory
  - …
- Widely used deployed systems
  - Tor (non-for-profit), initially funded by the NRL
  - Censorship resistant communications are playing an important role for fostering democracy and protecting people towards abusive states