ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

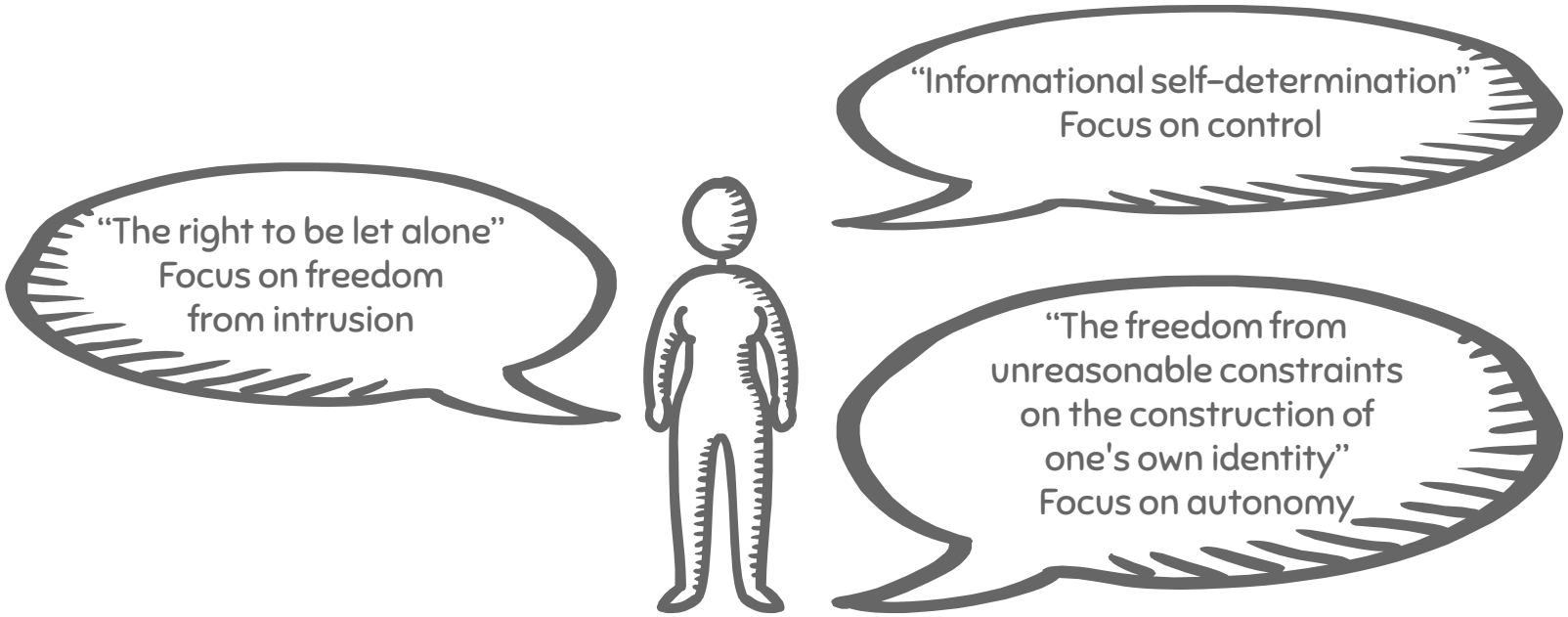
# Information Security and Privacy (COM-402)

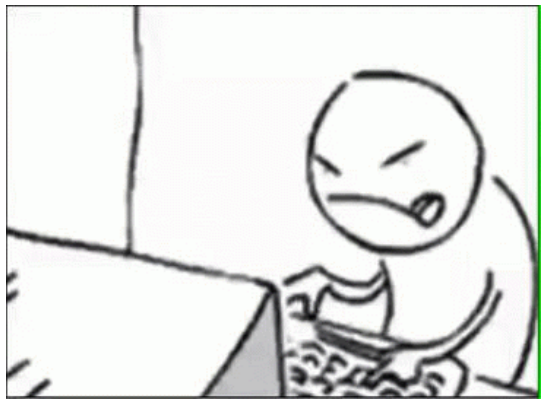
## Part 3: Privacy properties and privacy evaluation

**Carmela Troncoso**
SPRING Lab
carmela.troncoso@epfl.ch

Some slides/ideas adapted from: George Danezis, Bart Preneel, Claudia Diaz, Seda Guerses, JP Hubaux, Bryan Ford

# Anti-surveillance PETs – let's work on them!



**We can't design / program / evaluate these!!!?!?!?!?**

# Anti-surveillance PETs – technical goals

## Privacy properties

Confidentiality (in transit/storage, during processing)

Pseudonymity

Anonymity

Unlinkability

Unobservability

Plausible deniability

Game-oriented definitions
cryptographic definitions

and CS-523

and COM-501

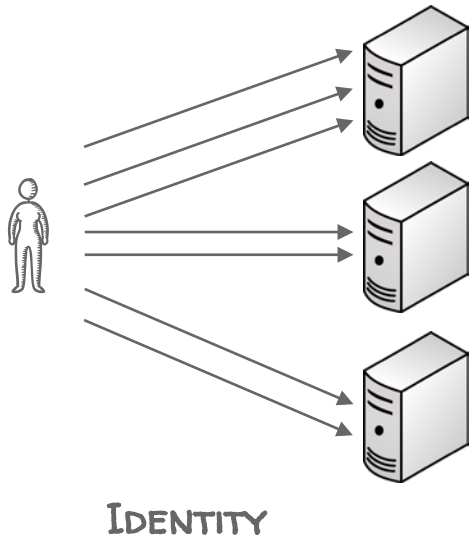
COM-402

# Anti-surveillance PETs – technical goals

## Privacy properties: **Pseudonymity**

**-Pfitzmann-Hansen**: “the use of pseudonyms as IDs [...] A digital pseudonym is a bit string which is unique as ID and which can be used to authenticate the holder”

**-ISO 15408**: “a user may use a resource or service without disclosing its identity, but can still be accountable for that use.”

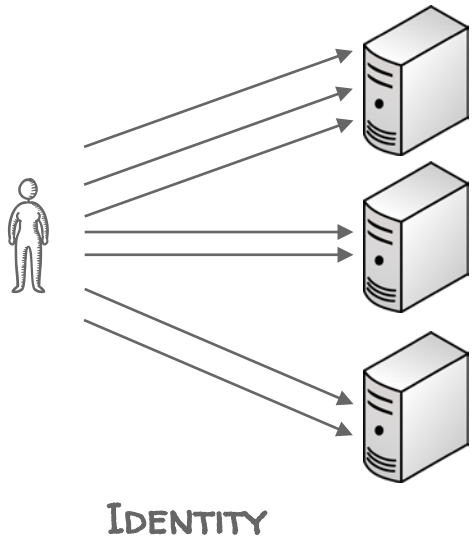


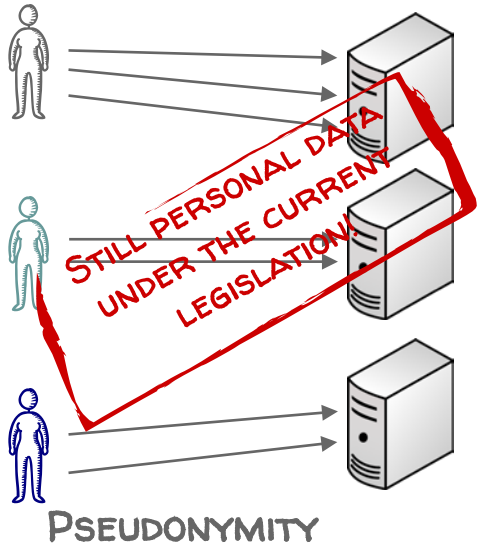
# Anti-surveillance PETs – technical goals

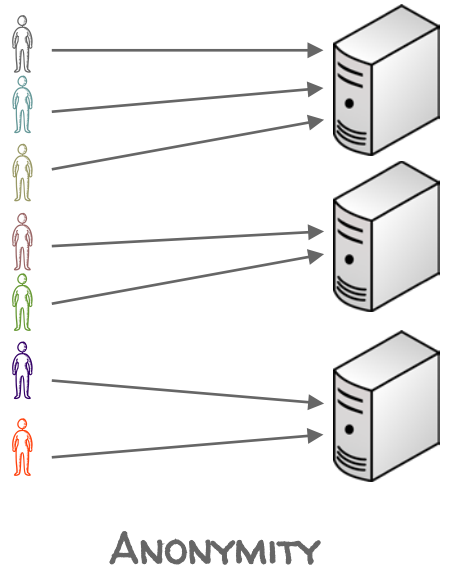
## Privacy properties: **Pseudonymity**

**-Pfitzmann-Hansen**: "the use of pseudonyms as IDs [...] A digital pseudonym is a bit string which is unique as ID and which can be used to authenticate the holder"

**-ISO 15408**: "a user may use a resource or service without disclosing its identity, but can still be accountable for that use."




Pfitzmann, Andreas and Hansen, Marit. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010.

# Example of pseudonymity technologies

- Use of persistent random identifiers
- Use of hashed identifiers
- Emails
- Nicknames

**These technologies are very limited from a privacy perspective, more later**

- Pseudo-identifiers

# Anti-surveillance PETs – technical goals

## Privacy properties: **Anonymity**

**-Pfitzmann-Hansen**: “Anonymity is the state of being not identifiable within a set of subjects, the anonymity set [...] The anonymity set is the set of all possible subjects who might cause an action”

**-ISO 29100**: “a characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly”

Who is...

...the reader of a web page, the person accessing a service
...the sender of an email, the writer of a text
...the person to whom an entry in a database relates
...the person present in a physical location

**DECOUPLING IDENTITY AND ACTION!**

# Anti-surveillance PETs – technical goals

## Privacy properties: **Unlinkability**

**-Pfitzmann-Hansen**: "two or more items within a system, are no more and no less related than they are related concerning the a-priori knowledge"

– **ISO15408**: " a user may make multiple uses of resources or services without others being able to link these uses together "

Two...

... anonymous letters written by the same person
... web page visits by the same user
… entries in a databases related to the same person
… two people related by a friendship link
… same person spotted in two locations

**DECOUPLING TWO ACTIONS FROM ONE USER!**

# Anti-surveillance PETs – technical goals

## Privacy properties: **Unobservability**

– **Pfitzmann-Hansen**: "an items of interest being indistinguishable from any item of interest at all […] Sender unobservability then means that it is not noticeable whether any sender within the unobservability set sends."

– **ISO15408:** "a user may use a resource or service without others, especially third parties, without being able to observe that the resource or service is being used."

Hiding...

...whether someone is accessing a web page
...whether a message is being sent
...whether an entry in a database corresponds to a real person
...whether someone or no one is in a given location
...

**DECOUPLING OBSERVATION FROM ACTION EXISTENCE!**

# Anti-surveillance PETs – technical goals

## Privacy properties: **Plausible Deniability**

– Not possible to prove user knows, has done or has said something
  – Resistance to coercion: one can always claim one does not know
  – Resistance to profiling: one cannot filter the fake entries

Not possible to prove ...
  ... that a person has hidden information in a computer
  ... that someone has the combination of a safe
  … that a person has been in a place at a certain point in time
  … that a database record belongs to a person

**DECOUPLING OBSERVATION FROM TRUE ACTION!**

# Systematic Privacy Evaluation

Confidentiality (in transit/storage, during processing)

Pseudonymity

Anonymity

Unlinkability

Unobservability

Plausible deniability

# Systematic Privacy Evaluation

Confidentiality (in transit/storage, during processing)

Cryptographic proofs

Pseudonymity

Anonymity

Unlinkability

Unobservability

Plausible deniability

# Systematic Privacy Evaluation

Confidentiality (in transit/storage, during processing)

Cryptographic proofs

Pseudonymity

Anonymity

Unlinkability

Unobservability

Plausible deniability

**Probabilistic analysis**

Anonymity - Pr[identity → action | observation ]

Unlinkability - Pr[action A ↔ action B | observation ]

Unobservability - Pr[real action |observation]

Plausible deniability - Pr[ fake| observation ]

# Systematic Privacy Evaluation

Confidentiality (in transit/storage, during processing)

Cryptographic proofs

Pseudonymity

Anonymity

Unlinkability

Unobservability

Plausible deniability

## Probabilistic analysis

Anonymity - Pr[identity → action | observation ]

Unlinkability - Pr[action A ↔ action B | observation ]

Unobservability - Pr[real action |observation]

Plausible deniability - Pr[ fake| observation ]

**Many times we use obfuscation as a means to achieve these properties**

Obfuscation - Pr[ real value| obfuscated value ]

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

2) Determine what the adversary will see

   Threat model: who is the adversary? what is the “observation”? what is her prior knowledge?

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

2) Determine what the adversary will see

   Threat model: who is the adversary? what is the "observation"? what is her prior knowledge?

3) "Invert" the mechanism as the adversary would do

   Always assume the adversary **knows** the mechanism and would try to undo its effect

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

2) Determine what the adversary will see

   Threat model: who is the adversary? what is the "observation"? what is her prior knowledge?

3) "Invert" the mechanism as the adversary would do

   Always assume the adversary **knows** the mechanism and would try to undo its effect

4) Evaluate property after inversion

   This is the real probability the adversary can compute

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

2) Determine what the adversary will see

   Threat model: who is the adversary? what is the "observation"? what is her prior knowledge?

3) "Invert" the mechanism as the adversary would do

   Always assume the adversary **knows** the mechanism and would try to undo its effect

4) Evaluate property after inversion

   This is the real probability the adversary can compute

**Anonymity** - Pr[identity → action | observation ]

**Unlinkability** - Pr[action A ↔ action B | observation ]

**Unobservability** - Pr[real action |observation]

**Plausible deniability** - Pr[ fake| observation ]

**Obfuscation** - Pr[ real value| obfuscated value ]

# Systematic Privacy Evaluation

1) Model the privacy-preserving mechanism as a probabilistic transformation

   What is the probability that, given an input the privacy mechanism returns a given output

2) Determine what the adversary will see

   Threat model: who is the adversary? what is the "observation"? what is her prior knowledge?

3) "Invert" the mechanism as the adversary would do

   Always assume the adversary **knows** the mechanism and would try to undo its effect

4) Evaluate property after inversion

   This is the real probability the adversary can compute

5) Measure

   Non trivial!!

**Anonymity** - Pr[identity → action | observation ]

**Unlinkability** - Pr[action A ↔ action B | observation ]

**Unobservability** - Pr[real action |observation]

**Plausible deniability** - Pr[ fake| observation ]

**Obfuscation** - Pr[ real value| obfuscated value ]

# Measuring privacy

**Anonymity** - Pr[identity → action | observation ]

**Correctness (e.g., error) :**
given the distribution, what is the probability that the adversary does not guess correctly?

**Uncertainty (e.g., entropy):**
given the distribution, what is the uncertainty of the adversary on the answer?

**Accuracy (e.g., confidence intervals):**
given the distribution, and a guess, how certain is the adversary of his inference?

**Differential privacy-based**:
given the observation what is the bound on the information the adversary can gain

Next block!

# Takeaways

Privacy is an abstract concept, need technical definitions to build technologies

We formalize privacy as privacy properties

- You may need more than one property to capture your privacy objectives!

Privacy evaluation

- the adversary knows
- the adversary makes probabilistic inferences
- metrics consider probabilities as seen from the adversary