FinTech R&D Innovation Conference

SnT securityandtrust.lu

Transparency, Verifiability and Privacy

Dr Lenzini Gabriele

Senior Research Scientist, SnT

ApSIA

FinTech R&D Innovation Conference

January 19th, 2016

Chambre de Commerce, Luxembourg

uni.lu Université du Luxembourg

Prologo

General Data Protection Regulation (GDPR) is the awaited European piece of general legislation in data protection.

One certainty:

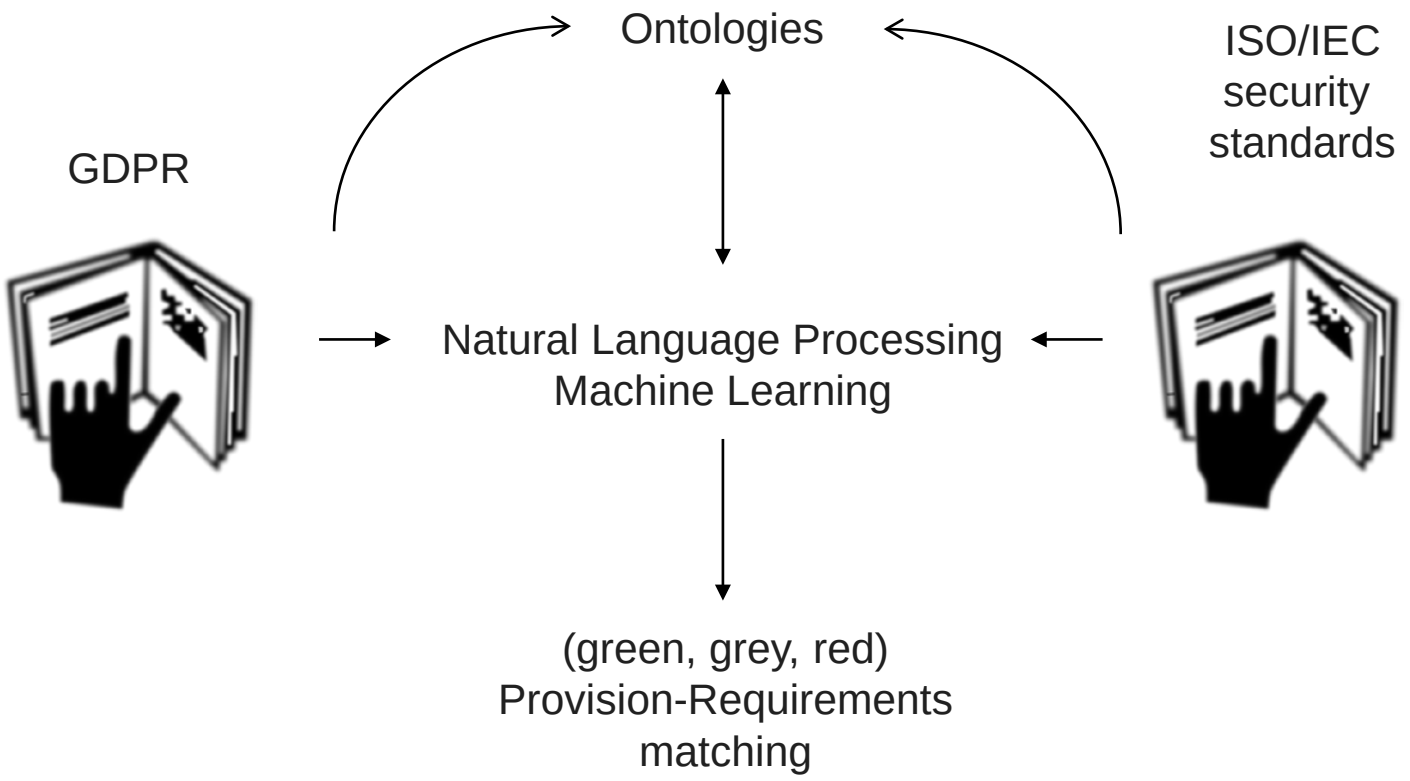
failure to comply → major financial losses
→ no more business for long

Research #1:
Data Privacy Requirements

Not to breach the GDPR, we need to be sure to adhere to data protection requirements.

This would be the role of (data privacy/protection) **standards**, certifications and auditors;

[But which ones among the plenty about security (e.g., ISO/IEC 27000), and what requirements for what provision?]



Interdisciplinary research: artificial intelligence, law and data protection regulators/

Challenge: Applying this research to Fintech and cloud computing

With: Dr. Bartolini, Dr. Giurgiu, Dr. Robaldo, and Prof. Cole

Research #2:
Transparency

Transparency, a general transversal principle, is believed to foster high quality of service provision.

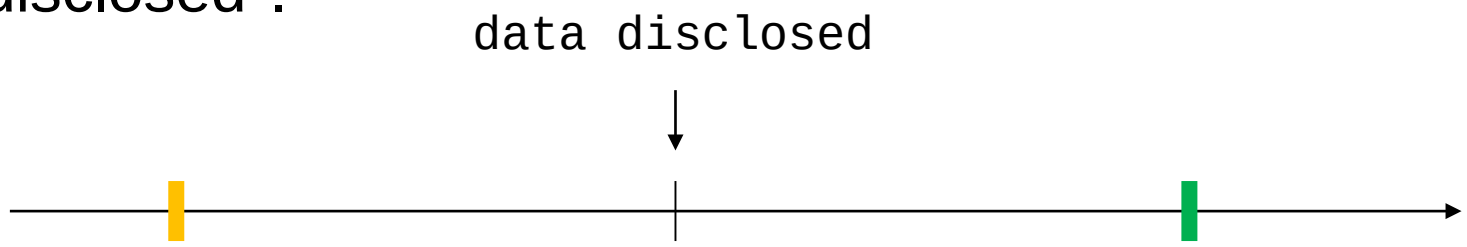
General Data Protection Regulation (GDPR) lists **transparency** as one of the driving (transversal) principles in processing personal data:

"data controllers are obliged to provide easily accessible information, [..] and procedures and mechanisms for exercising data subject's right"

Transparency: Definitions

[ex ante] - enables the anticipation of consequences before data are actually disclosed".

[ex post] – offers information about any consequences if data already have been revealed



≈ secure usability
(decision making)

≈ verifiability
(accountability/auditability)
≈ security design

Verifiability: basics

A **real system** (S)'s run (R), operated by agents (A^1,..,A^k) leaves traces, evidences (E).

They can be used to prove **security properties** about R.

One may want to check whether E,
even in the presence of malicious agents,
are enough to prove certain properties on R

Examples

e-Voting

- casted as voted
- counted as casted

e-Exams

- question secrecy
- mark anonymity

Concepts: Testable/Verifiable

A system is **testable** for a property P when it comes with (or allows) a test for a specific property

S is **verifiable** when T test is sound & complete

Test(E,S) ⇔ P holds on R

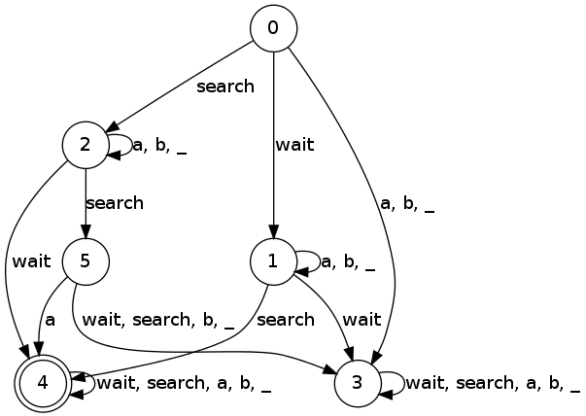
Universal **vs** Individual verifiability

Formalization

Real

System, Run, Evidences

Model



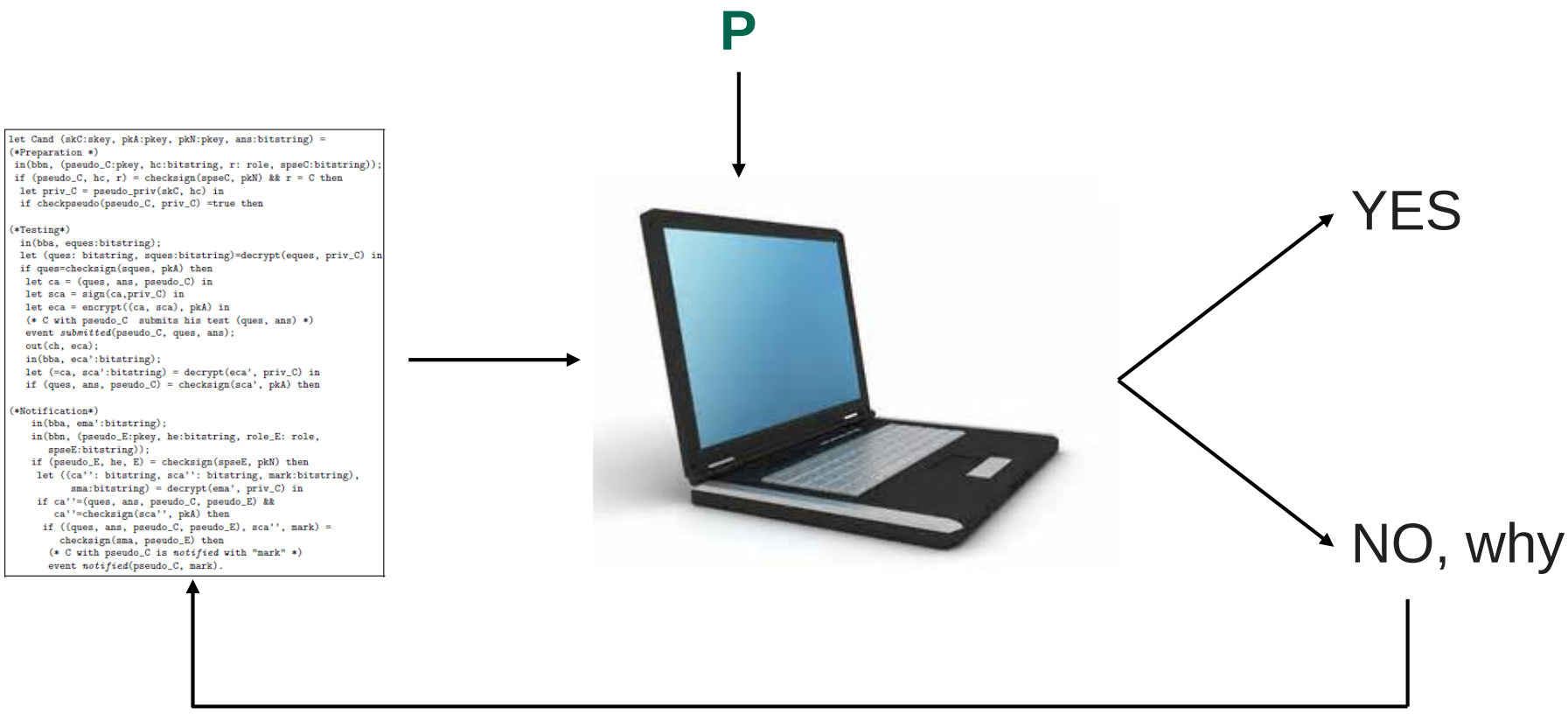
S $(A^1,..,A^k,I)$, *R*, *E* and *P*

We work with **formal models**

Examples

Requirement	Individual Verifiability	Universal Verifiability
Registration		$\mathtt{R}_{\mathtt{UV}}(e) \Leftrightarrow$ $I_r \supseteq \{i : (i,x) \in \mathtt{Accepted}\}$
Question Validity	$\mathtt{QV}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow (q \in Q_g)$	
Marking Correctness	$\mathtt{MC}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow$ $(\mathtt{Correct}(q,a) = m)$	$\mathtt{MC}_{\mathtt{UV}}(e) \Leftrightarrow$ $(\forall (i,x,m) \in \mathtt{Marked},$ $\mathtt{Correct}(x) = m$
Test Integrity	$\mathtt{ETI}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow$ $\big((i,(q,a)) \in \mathtt{Accepted}$ $\wedge \exists m' : (i,(q,a),m') \in \mathtt{Marked}\big)$	$\mathtt{ETI}_{\mathtt{UV}}(e) \Leftrightarrow \mathtt{Accepted} =$ $\{(i,x) : (i,x,m) \in \mathtt{Marked}\}$
Test Markedness	$\mathtt{ETM}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow$ $(\exists m' : (i,(q,a),m') \in \mathtt{Marked}))$	$\mathtt{ETM}_{\mathtt{UV}}(e) \Leftrightarrow \mathtt{Accepted} \supseteq$ $\{(i,x) : (i,x,m) \in \mathtt{Marked}\}$
Marking Integrity	$\mathtt{MI}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow$ $\exists m' : \big((i,(q,a),m') \in \mathtt{Marked}$ $\wedge (i,m') \in \mathtt{Assigned}\big)$	$\mathtt{MI}_{\mathtt{UV}}(e) \Leftrightarrow \mathtt{Assigned} =$ $\{(i,m) : (i,x,m) \in \mathtt{Marked}\}$
Marking Notification Integrity	$\mathtt{MNI}_{\mathtt{IV}}(i,q,a,m,p) \Leftrightarrow$ $(i,m) \in \mathtt{Assigned}$	

Automated Verifiability



We use **tools** to check whether a system has enough evidence to prove **P** even when malicious parties can compromised R

Examples

Requirement	Soundness	Completeness
Question Validity	✓ (EA)	✓(all)
Test Integrity	✓	✓(all)
Test Markedness	✓	✓(all)
Marking Correctness	✓ (EA)	✓(all)
Mark Integrity	✓	✓(all)
Mark Notification Integrity	✓	✓(all)

With: Dr. Giustolisi, and Prof. Ryan,

Towards Private Verifiability

Tests should have the minimal information disclosure and run on encrypted evidences enc(E),
without decrypting them
(e.g., using functional encryption)

With: Dr. Giustolisi, Dr. Iovino, and Prof. Ryan,

Towards verifiable Fintech protocols

Challenges: identifying security property relevant for Fintech; modelling and design Fintech verifiable protocols.

(e.g. verifiable authenticated transactions = all transactions are authenticated)

FinTech R&D Innovation Conference

SnT securityandtrust.lu

Thanks

for questions contact:

lenzini.gabriele@uni.lu

uni.lu Université du Luxembourg