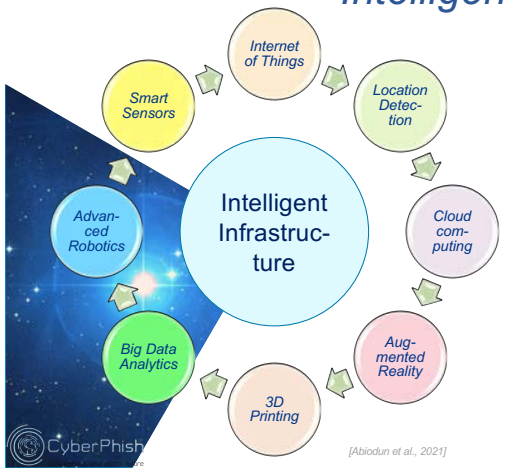
On Security of Intelligent Infrastructures

Raimundas Matulevičius

Institute of Computer Sciences
University of Tartu

https://infosec.cs.ut.ee/

Intelligent Infrastructure Systems



Complex socio-technical systems enabled by interconnected applications of the Internet of Things

[Abiodun et al., 2021]

Internet of Things

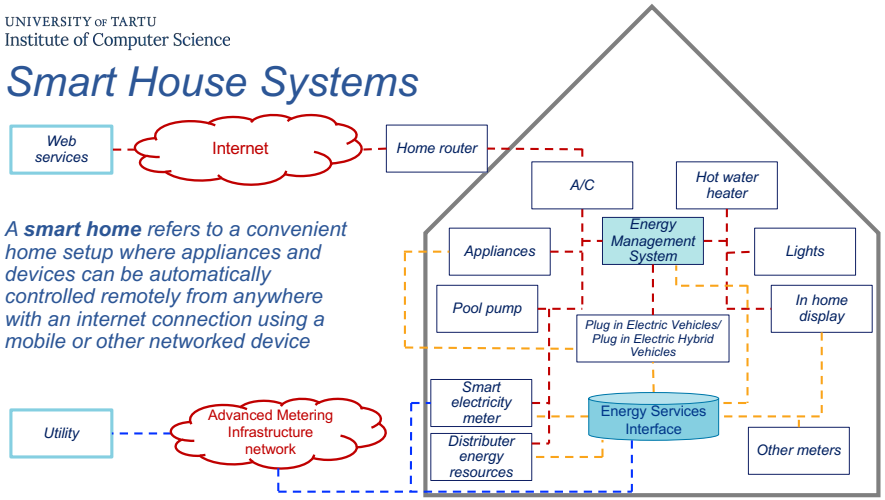
Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet

- *The "things", i.e., technologies, devices, objects, animals , or humans*
- *The networks of communication that connect the device*
- *The computer networks through data streaming from Internet to device*

Year	***World Population*** (*in billion*)	***IoT Connected Devices*** (*in billion*)	***Ratio***
2003	6,3	0,5	0,08
2010	6,8	12,5	1,84
2015	7,2	25	3,47
2020	7,6	50	6,58

[Abiodun et al., 2021]

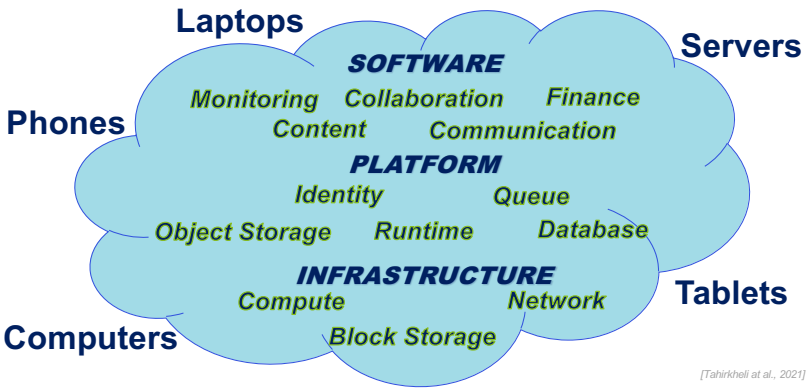
Smart House Systems



*A **smart home** refers to a convenient home setup where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device*

[Komninos et al., 2014]

Cloud Computing



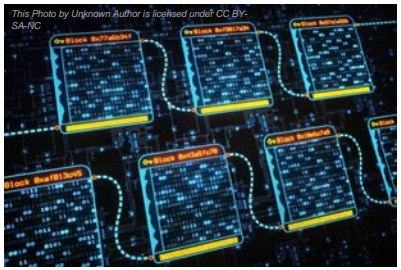
[Tahirkheli al al., 2021]

Big Data Ecosystem

	CHALLENGES
HUMAN *Business, Information, Social, Professional*	Lack of Consent, Social Misuse of Knowledge, Unauthorised Access, Data Deluge, Inappropriate Analytics, Availability, Accuracy
TECHNOLOGY *Application, Platform, Data Infrastructuure*	Multiple Uses of Data, Technology Gap, Agreed Data Usage, data, Timeliness, Data Provenance, Device Heterogeneity, Availability, Data Collection management & transfer, Data types and formats, Incomplete & Inconsistent data
FACILITY *Spatial, HVAC, Energy, Anciliary*	Storage and Processing Diverse Data Sources, Availability
ENVIRONMENT *Political, Environmental, Social, Technological, Legal*	Lack of Governance, Policies, Laws, Organisational Resistance, Establishing data driven culture

[Anwar et al., 2021]

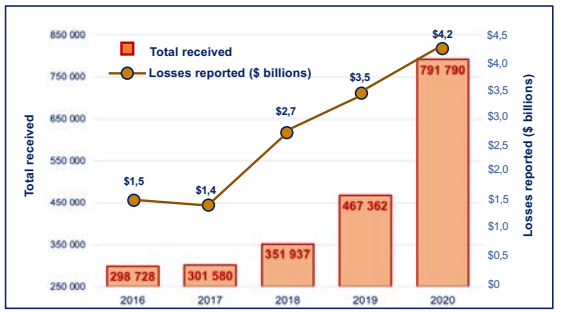
Blockchain Technology



Blockchain is a distributed immutable ledger technology, which gives participants an ability to share a ledger by peer-to-peer replication and updates every time when a transaction occurs

[Lewis , 2015; Sato and Himura, 2018]

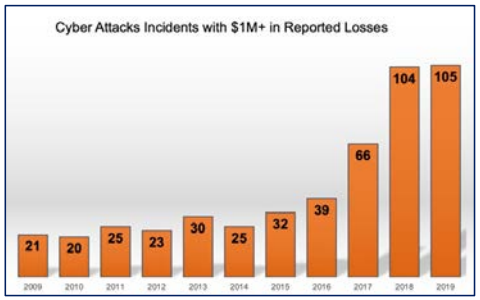
Growth of Cybersecurity Attacks

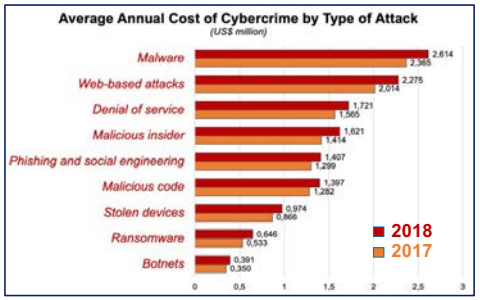


https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/?sh=17cfbc8c5fa2

Targeting people
Doing the homework
It is a numbers game
Scams keep evolving
Criminals sell stolen information
Patience and persistence pay off
Criminals can operate from anywhere

Cost of Cybersecurity Attacks





Over the past decade – **490** significant cyber incidents

2018 total = US$ **13** million

https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/ https://www.digitalmarketingcommunity.com/researches/ninth-annual-cost-of-cybercrime-research-2019/

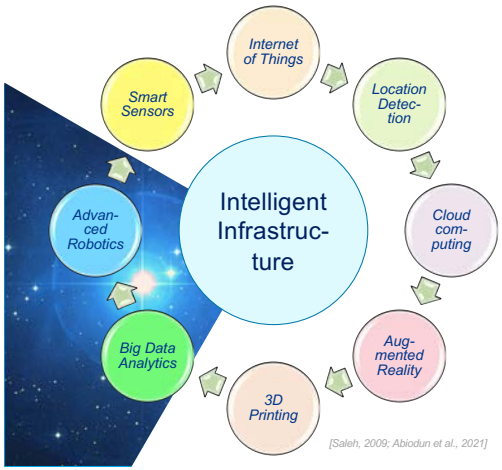
Top Most Common Security Attacks

Top Most Common Security Attacks

2021	2022
1. Malware	1. Malware
2. Phishing	2. Phishing
3. DDOS	3. MitM
4. MitM	4. DDOS
5. Credential Stuffing	5. SQL injection
6. Password Spraying	6. Zero-day Exploit
7. Mobile Device	7. Password Spraying
…	…

https://auth0.com/blog/the-7-most-common-types-of-cybersecurity-attacks-in-2021/
https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

Wide Use of Technology



[Saleh, 2009; Abiodun et al., 2021]

- Trustworthy System
  - *"a system that gains a high level of trust by its users by satisfying the specified security, privacy, safety, availability and business integrity requirements"*
- The need to secure information becomes a necessity than an option

Table of Contents

ITS: Intelligent Transportation Systems

- ***Security Risk Management***
- *Management of Personal Information*
- *Management of Forensic Evidence*

How to manage security risks in ITS?

Intelligent Transportation Systems

Apply information, communication, and sensor technologies to vehicles and transportation infrastructure

Provide real-time information for road users and transportation system operators to make better decisions

https://www.sciencedirect.com/topics/engineering/intelligent-transportation-system
http://www.nexcom.com/news/Detail/intelligent-transportation-systems-world

Intelligent Transportation Systems

- People counting
- First aid / response
- Scheduling
- Transit surveillance
- Toll collection
- Automatic number-plate recognition

http://www.nexcom.com/news/Detail/intelligent-transportation-systems-world

Security Engineering

Lowering the
risk of intentional unauthorized harm
to valuable assets to level
that is acceptable to the system's
stakeholders by preventing and reacting to
malicious harm, misuse, threats,
and security risks

Different from safety

Values must be protected

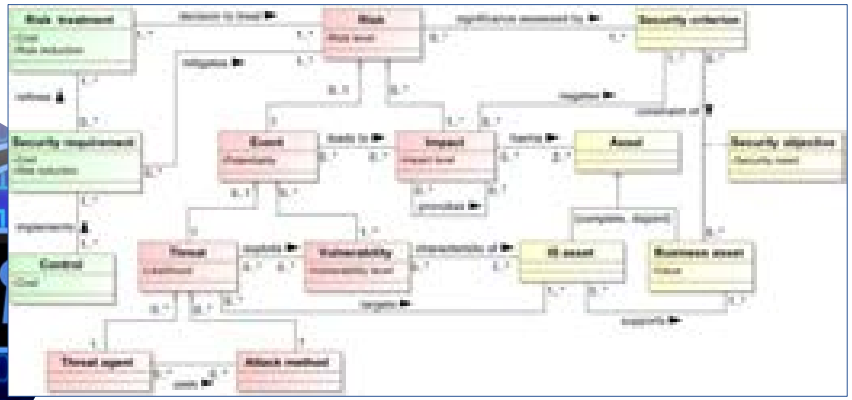
There no 100% security

Different risk forms

Firesmith, D.: Engineering safety- and security-related requirements for software- intensive systems. Tutorial, 2007 Carnegie Mellon University (2007)

Information Systems

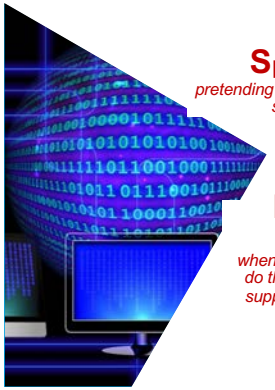
Security Risk Management



Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management, pp. 289–306. Springer, New York (2010)

UNIVERSITY OF TARTU
Institute of Computer Science

Security Threat Analysis



STRIDE

Spoofing:
pretending to be something or someone

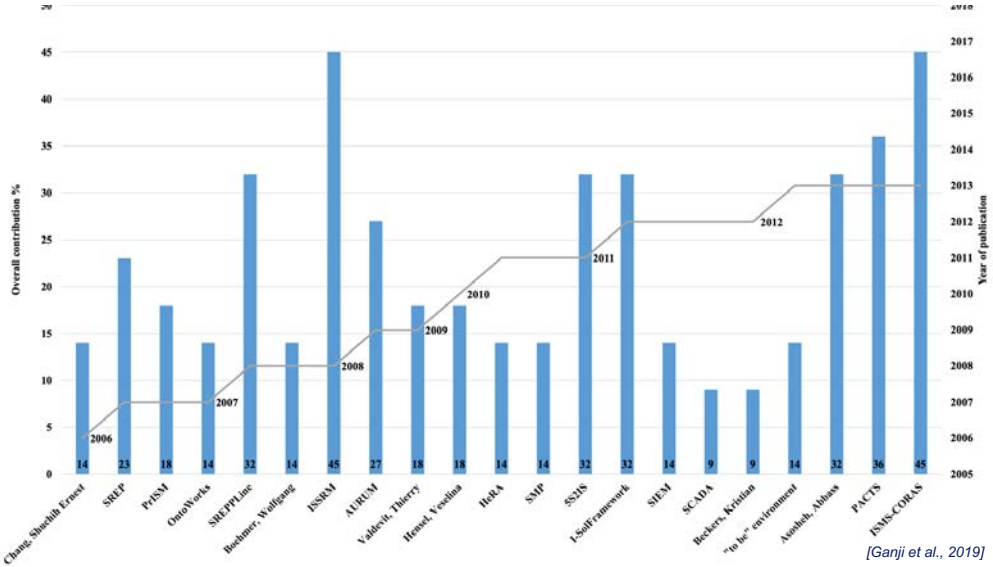
Tampering:
modifying something that you are not supposed to modify

Repudiation:
claiming you didn't do something (regardless of if this is true or not)

Elevation of privilege:
when program or usage can do things that they are not supposed to be able to do

Information disclosure:
exposing information to whose who are not authorizes to view it

Denial of service:
attacks to prevent a system from providing its intended service by crashing, slowing down or filling its storage



[Ganji et al., 2019]

UNIVERSITY OF TARTU
Institute of Computer Science

Security treatment

Security Requirements

Integrity
*Extent to which a system shall ensure that its data and communications **are not intentionally corrupted** via unauthorised creation, modification, or deletion*

Authentication
*Extent to which a system shall **verify** the identity of its externals before interacting with them*

Non-repudiation
*Extent to which a system shall prevent a party to one of its interactions from **denying having participated** in all or part of the interaction*

Authorization
*Specifies the **access and usage** privileges of authenticated users*

Availability
*Extend to which system and data remains **available** for the user*

Confidentiality
Extend to which system is able to identify and verify externals, and grant them access to data and services

UNIVERSITY OF TARTU
Institute of Computer Science

Intelligent Transportation Systems

PERCEPTION LAYER
Sensing | Vision | Positioning | Actuating

NETWORK LAYER
In-Vehicle | Vehicle to Vehicle | Vehicle to Infrastructure

APPLICATION LAYER
Computing/ Server | Data Storage | Human

Affia A-a. O., Matulevičius R., Nolte A.: Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review. Panetto H. *et al.* (eds.), LNCS 11877, CoopIS 2019, Springer

Intelligent Transportation Systems

Perception Layer

	Sensing	Vision	Positioning	Actuating
System Assets	Thermometer	Video cameras	Global positioning system (GPS) receiver	Engine control unit (ECU)
supports				
Business Assets	Heat measurement	Traffic count	Pseudo-range measurement Vehicle location data	Event data records

Intelligent Transportation Systems

Perception Layer

	SECURITY THREATS					
System Assets	***S**poofing*	***T**ampering*	***R**epudiation*	***I**nformation disclosure*	***D**enial of service*	***E**levation of privileges*
Sensing, Positioning, Vision technologies	Spoofing, Node impersonation, Illusion, Replay, Sending deceptive messages, Masquerading	Forgery, Data manipulation, Tampering, Falsification of readings, Massage injection	Bogus message	Stored attacks, Eavesdropping	Message saturation, Jamming, Denial of service (DoS), Disruption of system	Backdoor, Unauthorized access, Malware, Elevation of privilege, Remote update of ECU
Total (occurrences)	**6(15)**	**5(6)**	**1(1)**	**2(2)**	**5(6)**	**5(6)**

Intelligent Transportation Systems

Perception Layer

(Integrity)
Restricted physical access, Challenge/response mechanism, Use trusted hardware piratically impossible to alter existing values unless authorised

(Authentication)
Spoofing resistant positioning system, Devise level user authentication, Digital certificates, Digital signature of software and sensors, Challenge/ response mechanism, Encrypted precise positioning system

(Non-repudiation)
Use trusted hardware piratically impossible to alter existing values unless authorised

Security controls

(Confidentiality)
Encryption

(Authorization)
Threat modelling, Hardware and software access control, Uupgrading on-board diagnostics (OBD)-II port

(Availability)

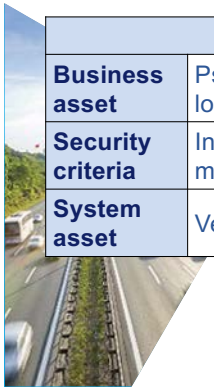
Lesson Learnt

Risk-related concepts are not treated in the right granularity

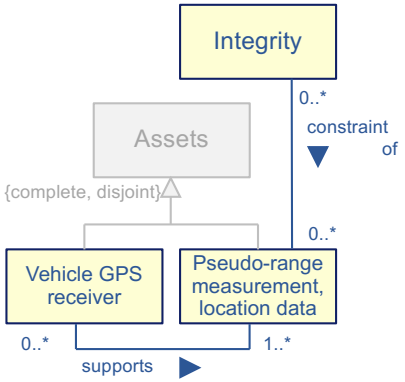
- Cause of risk ≠ threat
- Consequences of risk on asset security criterion

Intelligent Transportation Systems

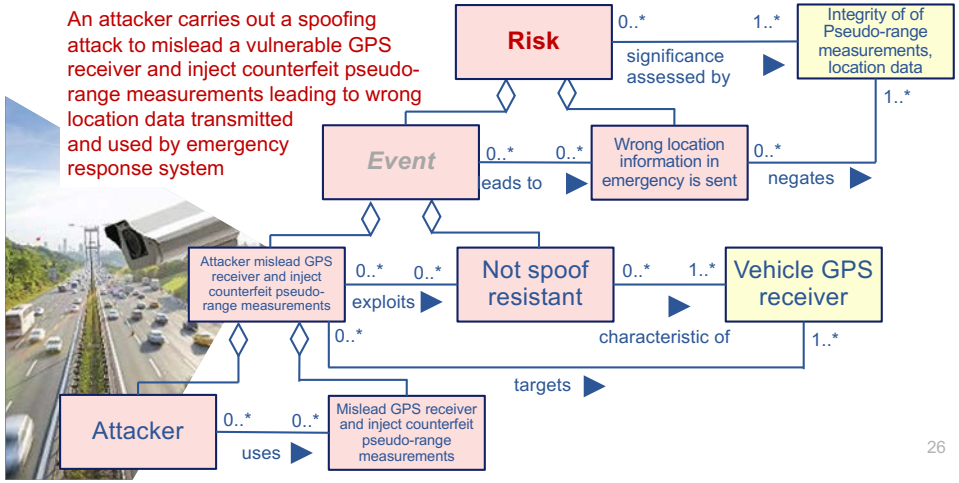
Perception Layer



Positioning	
Business asset	Pseudo-range measurements, location data
Security criteria	Integrity of Pseudo-range measurements, location data
System asset	Vehicle GPS receiver



An attacker carries out a spoofing attack to mislead a vulnerable GPS receiver and inject counterfeit pseudo-range measurements leading to wrong location data transmitted and used by emergency response system



Lesson Learnt

ITS layers – Security attacks and impact

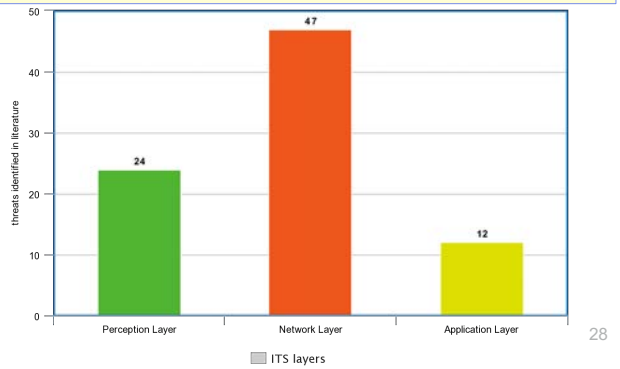
PERCEPTION LAYER			
Sensing	Vision	Positioning	Actuating

NETWORK LAYER		
In-Vehicle	Vehicle to Vehicle	Vehicle to Infrastructure

APPLICATION LAYER		
Computing/ Server	Data Storage	Human

Lesson Learnt

Network layer threats have seen a lot of research focus



Other Examples

Security Risk Management in Vehicle's **Architecture**

- A.-A. O. Affia, R. Matulevicius, R.Tõnisson (2021) Security Risk Estimation and Management in Autonomous Driving Vehicles. CAiSE Forum: 11-19

Security Risk Management at **Communication of Vehicle and Infrastructure**

- A-A. O. Affia, R. Matulevicius (2021): Securing an MQTT-based Traffic Light Perception System for Autonomous Driving. CSR 2021: 255-260

Vulnerabilities at **Mobility Systems**

- A-A. O. Affia, R. Matulevicius (2022): Security Risk Management in Shared Mobility Integration. ARES 2022: 145:1-145:10

Security Risk Management at **Passenger Vehicle Interaction**

- M. Bakhtina, R. Matulevicius (2022): Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 13(1): 87-111 (2022)

UNIVERSITY OF TARTU
Institute of Computer Science

Table of Contents

ITS: Intelligent Transportation Systems

- *Security Risk Management*
- ***Management of Personal Information***
- *Management of Forensic Evidence*

RQ1: How to define requirements for privacy assurance of the personal data according to GDPR?

RQ2: How to compare effectiveness of privacy-enhancing technologies in the context of the business process?

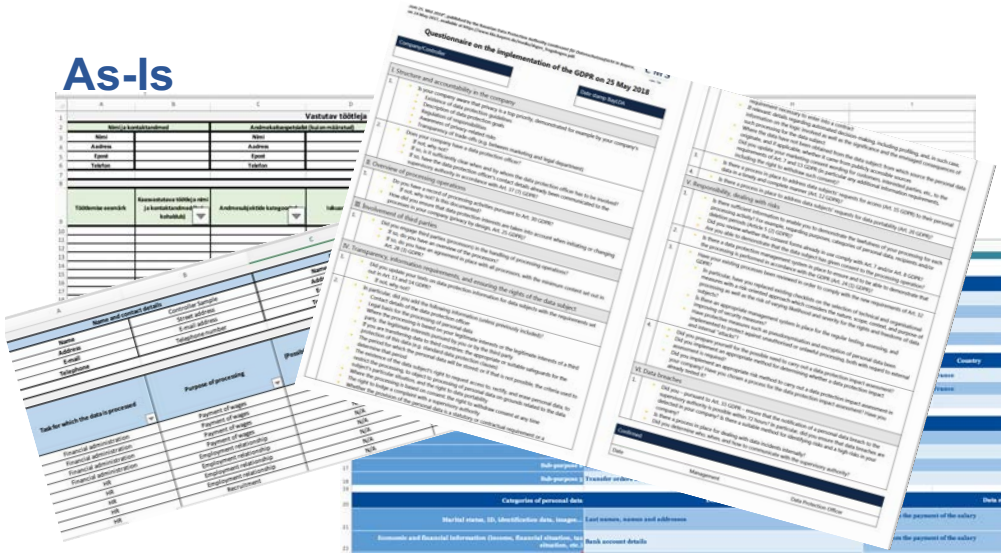
UNIVERSITY OF TARTU
Institute of Computer Science

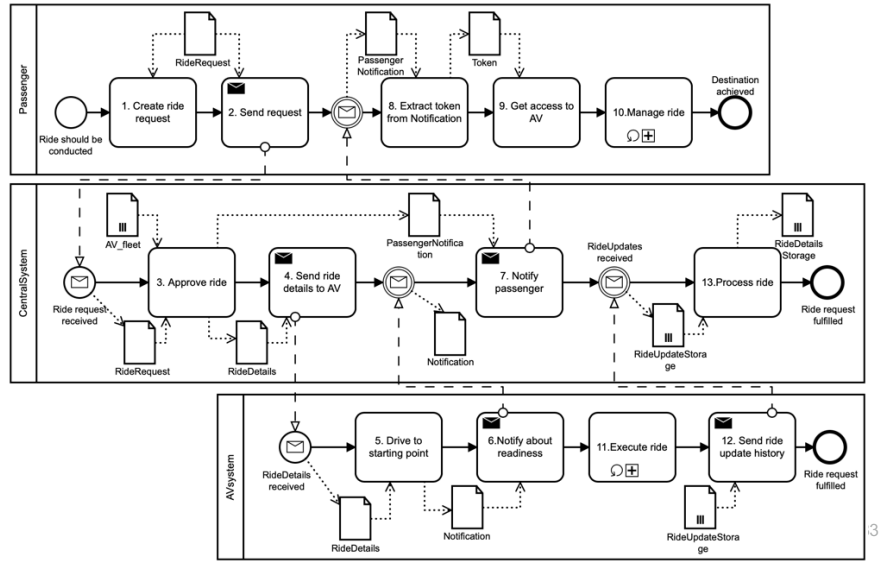
Motivation

- Organisations require techniques to assess and make compliant their state of the data processing
- Failing to meet compliance requirements may result in administrative fines

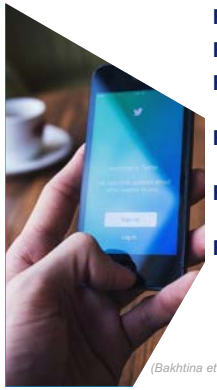
https://enforcementtracker.com/

As-Is





Requirements



(Bakhtina et al. 2021)

Req.1: **Passenger's location** should be available to the assigned AV

Req.2: Passenger can get access to the AV using the provided **Token**

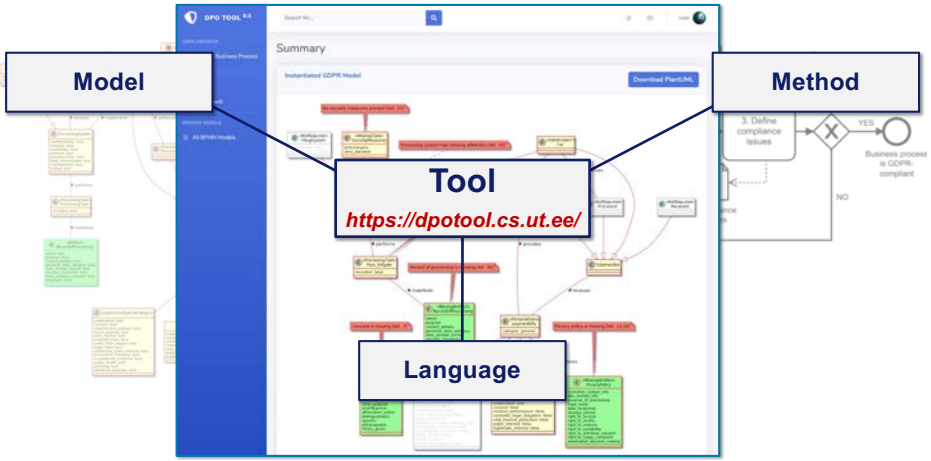
Req.3: Token should be generated based on the data from **Ride Request** and the assigned **AV details**

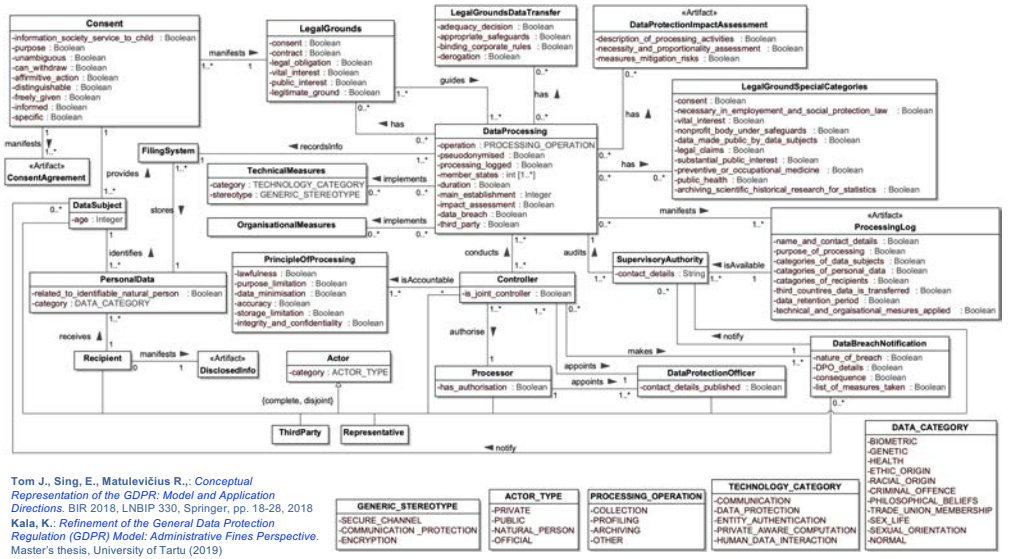
Req.4: Central System should process the **ride changes history** after the ride is finished

Req.5: Central System should not have access to the current **passenger's location** during the ride

Req.6: Central System and AV system are verified by one another and have the established secure connection

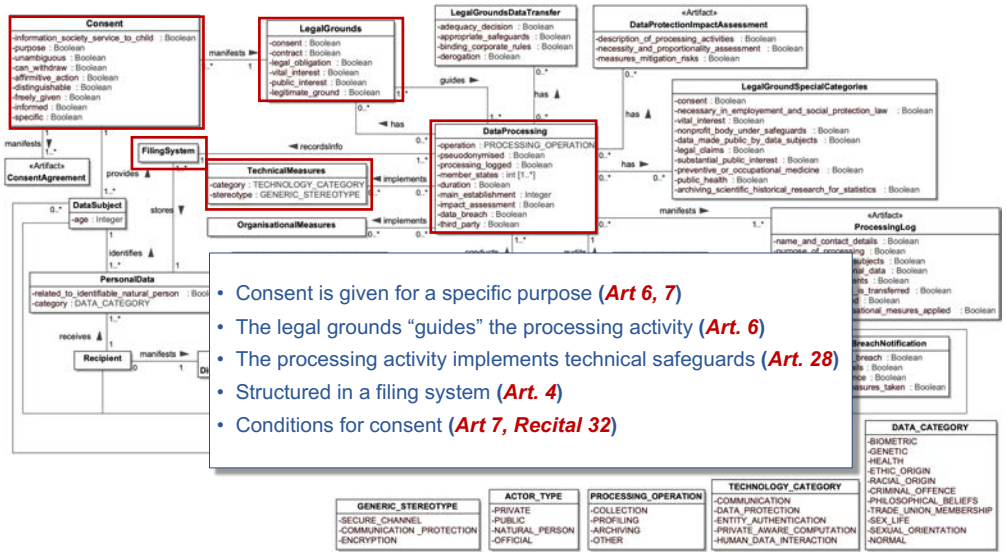
GDPR Compliance Analysis





Tom J., Sing, E., Matulevičius R.,: *Conceptual Representation of the GDPR: Model and Application Directions.* BIR 2018, LNBIP 330, Springer, pp. 18-28, 2018

Kala, K.: *Refinement of the General Data Protection Regulation (GDPR) Model: Administrative Fines Perspective.* Master's thesis, University of Tartu (2019)

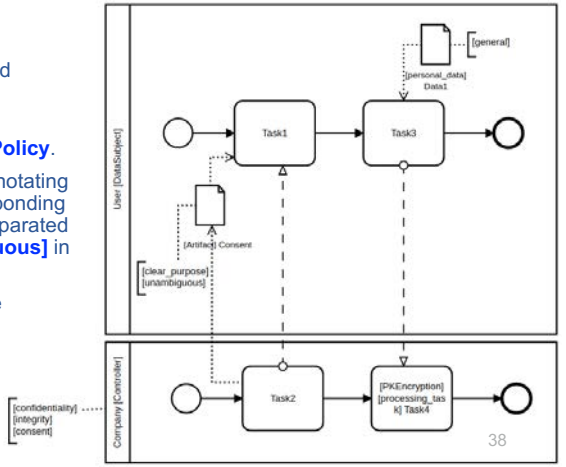


- Consent is given for a specific purpose (***Art 6, 7***)
- The legal grounds “guides” the processing activity (***Art. 6***)
- The processing activity implements technical safeguards (***Art. 28***)
- Structured in a filing system (***Art. 4***)
- Conditions for consent (***Art 7, Recital 32***)

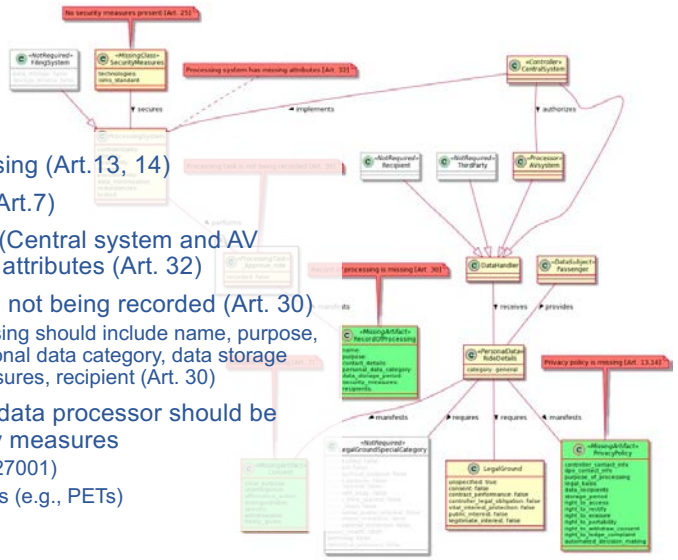
UNIVERSITY OF TARTU
Institute of Computer Science

Modelling Language

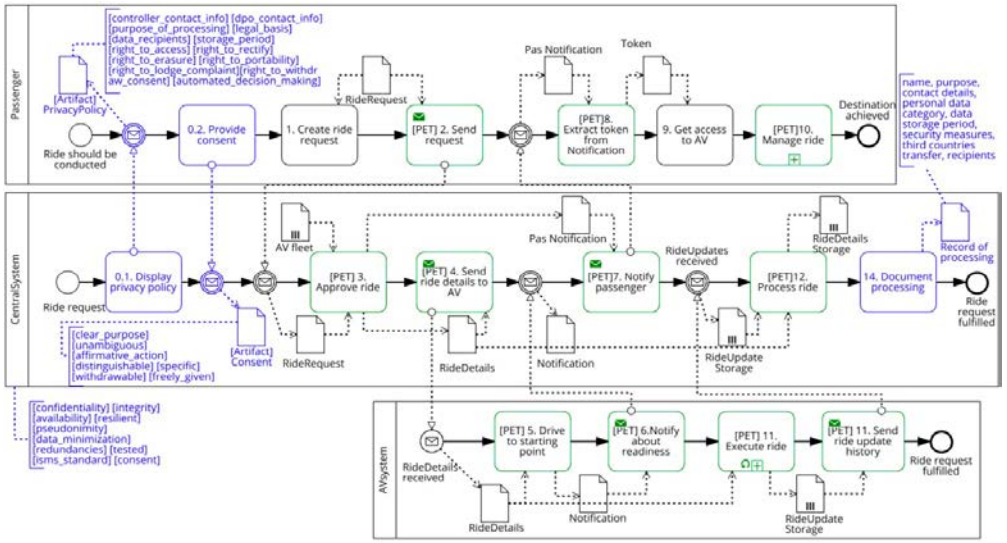
- Actors such as the controller are described using **Company [Controller]**.
- Artifacts are described using **[Artifact] Consent** or **[Artifact] PrivacyPolicy**.
- Attributes of artifacts are described by annotating the appropriate artifact with labels corresponding to the attributes. Multiple attributes are separated by a space - **[clear_purpose] [unambiguous]** in this case.
- Personal data is assigned by prefixing the appropriate data object label with the prefix **[personal_data]**
- …



UNIVERSITY OF TARTU
Institute of Computer Science



- Privacy policy is missing (Art.13, 14)
- Consent is missing (Art.7)
- Processing systems (Central system and AV system) has missing attributes (Art. 32)
- Processing tasks are not being recorded (Art. 30)
  - the record of processing should include name, purpose, contact details, personal data category, data storage period, security measures, recipient (Art. 30)
- Central system as a data processor should be secured with security measures
  - standards (e.g., ISO27001)
  - concrete technologies (e.g., PETs)



PETs: *Privacy Enhancing Technologies*

Technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals

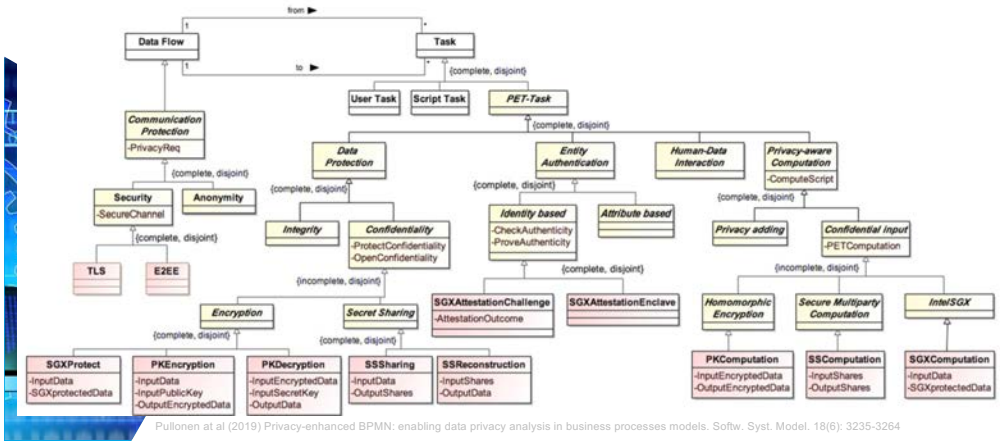
https://en.wikipedia.org/wiki/Privacy-enhancing_technologies

PETs Classification

Goal	Target	Example of technology
Communication protection	Security	Client-server encryption, TLS, IPSec, end-to-end encrypetion, PGP, OTR
	Anonymity	Proxies, VPN, onian routing, mix networks, broadcast
Data protection	Integrity	Message authentication codes, signatures
	Confidentiality	Encryption, secret sharing
Entity authentication	Identity-based	User names and passwords, single-sign-on
	Attribute-based	Credential used only once, zero-knowledge proofs
Privacy-aware computation	Confidential inputs	Homomorphic encryption, secure multiparty computation, Intel SGX
	Privacy adding	Differential privacy, k-anonymity, cell suppression, noise addition, aggregation, anonymisation
Human-data interaction	Transparency of data usage	Information flow detection, logging, declarations about information usage
	Intervenability	Information granularity adjustment, access control

(Danezis et al. 2015)

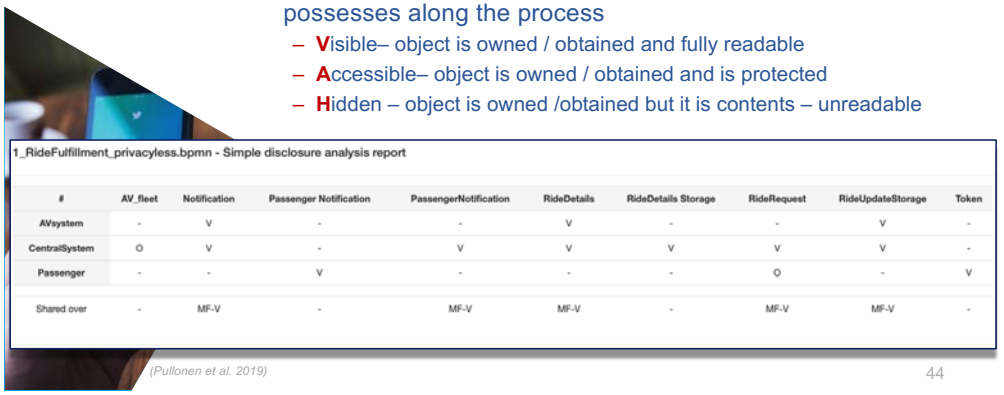
PE-BPMN abstract syntax



Pullonen at al (2019) Privacy-enhanced BPMN: enabling data privacy analysis in business processes models. Softw. Syst. Model. 18(6): 3235-3264

Visibility Matrix

- **Visibility matrix** – overview of data objects that each actor possesses along the process
  - **V**isible– object is owned / obtained and fully readable
  - **A**ccessible– object is owned / obtained and is protected
  - **H**idden – object is owned /obtained but it is contents – unreadable



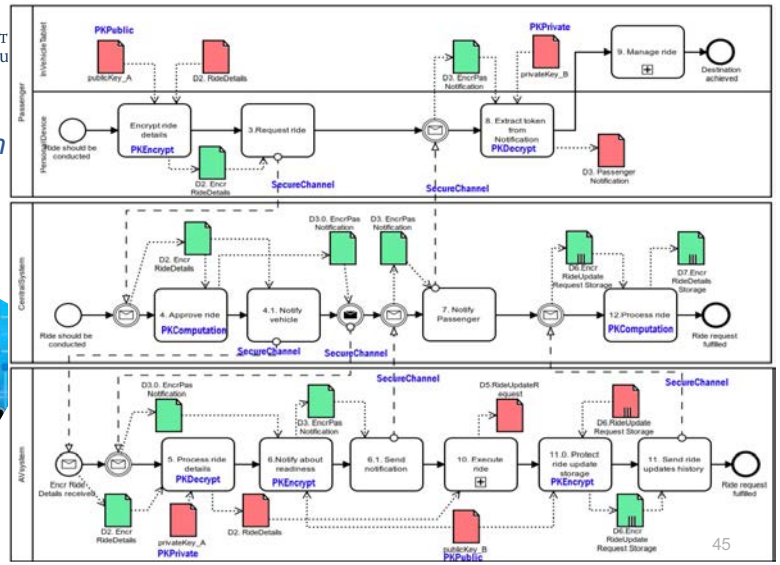
1_RideFulfillment_privacyless.bpmn - Simple disclosure analysis report

#	AV_fleet	Notification	Passenger Notification	PassengerNotification	RideDetails	RideDetails Storage	RideRequest	RideUpdateStorage	Token
AVsystem	-	V	-	-	V	-	-	V	-
CentralSystem	O	V	-	V	V	V	V	V	-
Passenger	-	-	V	-	-	-	O	-	V
Shared over	-	MF-V	-	MF-V	MF-V	-	MF-V	MF-V	-

(Pullonen et al. 2019)

UNIVERSITY OF TART
Institute of Compu

PKEncryption



(Bakhtina et al. 2021)

UNIVERSITY OF TART
Institute of Compu

PKEncryption

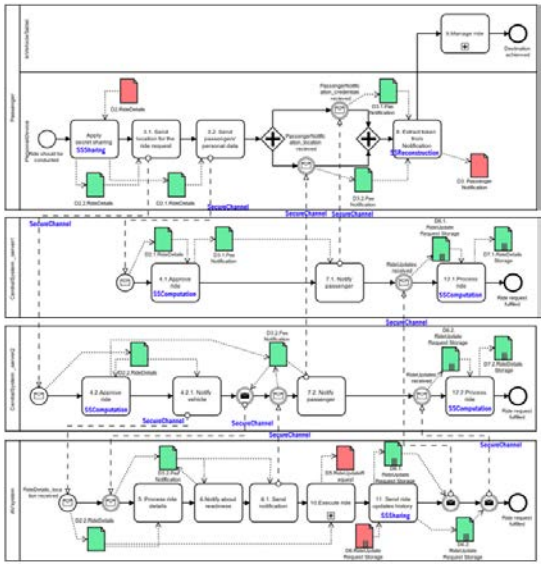
4_Pleak_RideFulfillmetn_PK_PE_BPMN.bpmn - Simple disclosure analysis report

#	AV_fleet	EncrRideDetailsStorage	IntermToken	EncrPasNotification, PasNotification	EncrRideDetails, RideDetails	EncrRideUpdateStorage, RideUpdateStorage	Token	[Artifact] RecordOfProcessing	[Artifact]Consent	EncrRideRequest, [personal_data]RideRequest
AVsystem [Processor]	-	-	H	H	V	V	-	-	-	-
CentralSystem [Controller]	O	H	H	H	H	H	-	V	V	H
Passenger [DataSubject]	-	-	-	H	-	-	V	-	-	O
Shared over	-	-	S	S	S	S	-	-	-	S

(Bakhtina et al. 2021)

UNIVERSITY OF TARTU
Institute of Computer Science

SSSharing



(Bakhtina et al. 2021)

UNIVERSITY OF TARTU
Institute of Computer Science

SSSharing

5_Pleak_RideFulfillmetn_SSharing_PE_BPMN.bpmn - Simple disclosure analysis report

#	RideDetails Storage_1, RideDetails Storage_2	RideUpdateStorage, RideUpdateStorage_1, RideUpdateStorage_2	Token, Token_1, Token_2	[Artifact] Consent	[Artifact] RecordOfProcessing	RideRequest_1, RideRequest_2, [personal_data]RideRequest	[Artifact] PrivacyPolicy
AVsystem [Processor]	-	V	H	-	-	H	-
CentralSystem[Controller]	H	H	H	V	V	H	-
External_server[Prcoessor]	H	H	H	-	-	H	-
Passenger [DataSubject]	-	-	V	-	-	O	-
Shared over	-	S	S	-	-	S	-

(Bakhtina et al. 2021)

4_Pleak_RideFulfillmetn_PK_PE_BPMN.bpmn - Simple disclosure analysis report

#	AV_fleet	EncrRideDetailsStorage	IntermToken	EncrPasNotification, PasNotification	EncrRideDetails, RideDetails	EncrRideUpdateStorage, RideUpdateStorage	Token	[Artifact] RecordOfProcessing	[Artifact]Consent	EncrRideRequest, [personal_data]RideRequest
AVsystem [Processor]	-	-	H	H	V	V	-	-	-	-
CentralSystem [Controller]	O	H	H	H	H	H	-	V	V	H
Passenger [DataSubject]	-	-	-	H	-	-	V	-	-	O
Shared over	-	-	S	S	S	S	-	-	-	S

- The same level of '**Ride Update Storage**' and '**Ride Details Storage**' visibility

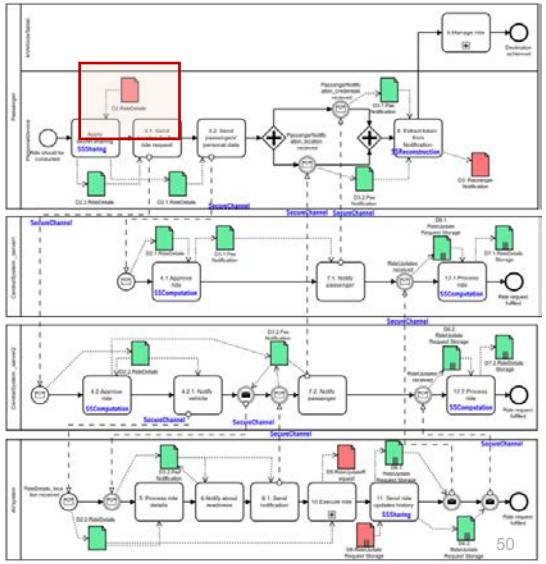
5_Pleak_RideFulfillmetn_SSharing_PE_BPMN.bpmn - Simple disclosure analysis report

#	RideDetails Storage_1, RideDetails Storage_2	RideUpdateStorage, RideUpdateStorage_1, RideUpdateStorage_2	Token, Token_1, Token_2	[Artifact] Consent	[Artifact] RecordOfProcessing	RideRequest_1, RideRequest_2, [personal_data]RideRequest	[Artifact] PrivacyPolicy
AVsystem [Processor]	-	V	H	-	-	H	-
CentralSystem[Controller]	H	H	H	V	V	H	-
External_server[Prcoessor]	H	H	H	-	-	H	-
Passenger [DataSubject]	-	-	V	-	-	O	-
Shared over	-	S	S	-	-	S	-

UNIVERSITY OF TARTU
Institute of Computer Science

SSSharing

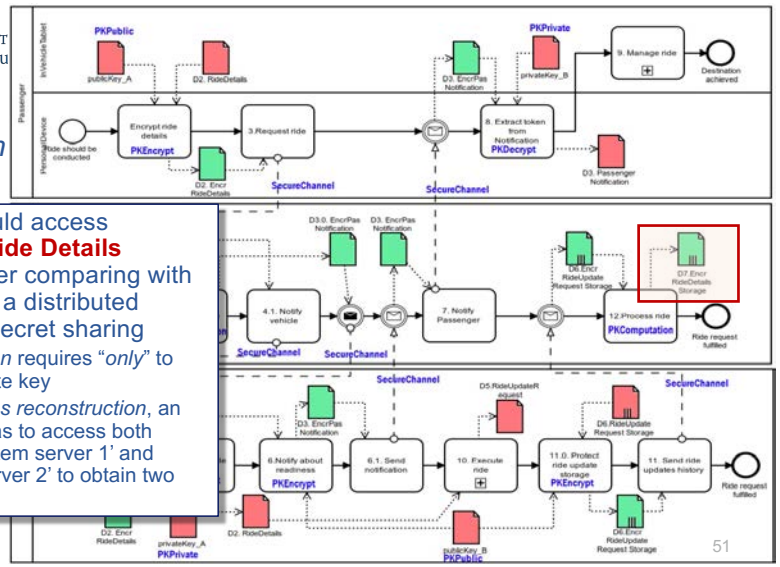
- *Secret sharing* for '**Ride Request**' imposes prerequisites to the passenger's device
  - It has minimum processing capabilities for conducting *secret sharing*
  - *Secret sharing* may increase the processing time of the Ride Fulfilment process
  - No feasible benefit in terms of better privacy protection



(Bakhtina et al. 2021)

UNIVERSITY OF TART
Institute of Compu

PKEncryption

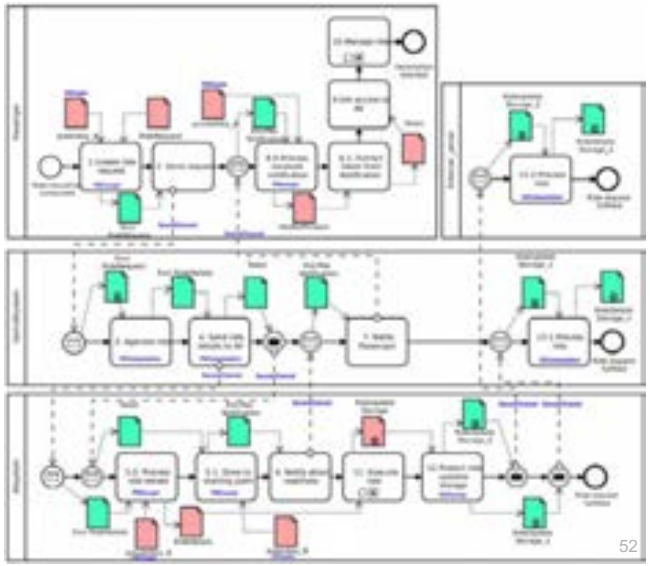


- Adversary could access '**Encrypted Ride Details Storage**' easier comparing with the storage in a distributed manner with secret sharing
  - *PK encryption* requires "*only*" to have a private key
  - *Secret shares reconstruction*, an adversary has to access both 'Central System server 1' and 'External Server 2' to obtain two shares

(Bakhtina et al. 2021)

UNIVERSITY OF TARTU
Institute of Computer Science

Combined design

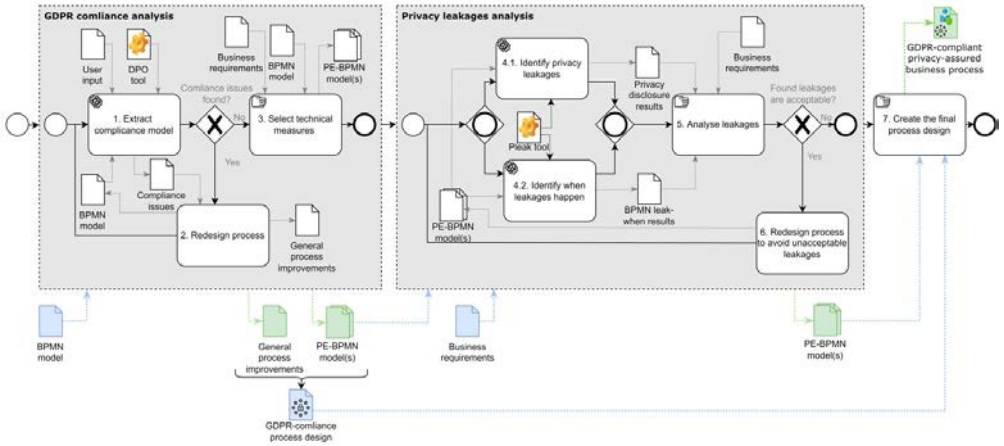


(Bakhtina et al. 2021)

Combined design

6_RideFulfillment_PK_SecSharing_combined.bpmn - Simple disclosure analysis report

#	IntermToken	EncrPas Notification, PasNotification	Encr RideDetails, RideDetails	RideDetails Storage_1, RideDetails Storage_2	Encr RideRequest, RideRequest	RideUpdate Storage, RideUpdate Storage_1, RideUpdate Storage_2	Token	privateKey_A	privateKey_B	publicKey_A	publicKey_B
AVsystem	V	V	V	-	-	V	-	O	-	-	O
CentralSystem	V	H	H	H	H	H	-	-	-	-	-
External _server	-	-	-	H	-	H	-	-	-	-	-
Passenger	-	V	-	-	O	-	V	-	O	O	-
Shared over	S	S	S	-	S	S	-	-	-	-	-



Other Examples

Privacy Preservation for **Vehicle Parking**

- P. Dzurenda, F. Jacques, M. Knockaert, M. Laurent, L. Malina, R. Matulevicius, Q. Tang, A. Tasidou (2022): Privacy-preserving solution for vehicle parking services complying with EU legislation. PeerJ Comput. Sci. 8: e1165

Managing Personal Data in **Vehicle Recharge Process**

- G. Roascio, G. Costa, E. Baccelli, L. Malina, R. Matulevicius, M. Momeu, N. Morkevicius, E. Russo, B. Stojanovic, A. Tasidou (2022): HArMoNICS: High-Assurance Microgrid Network Infrastructure Case Study. IEEE Access 10: 115372-115383

Managing Personal Data when **Vehicle Passing Tollgate**

- R. Matulevicius, J. Tom, K. Kala, E. Sing (2020): A Method for Managing GDPR Compliance in Business Processes. CAiSE Forum: 100-112

Table of Contents

ITS: Intelligent Transportation Systems

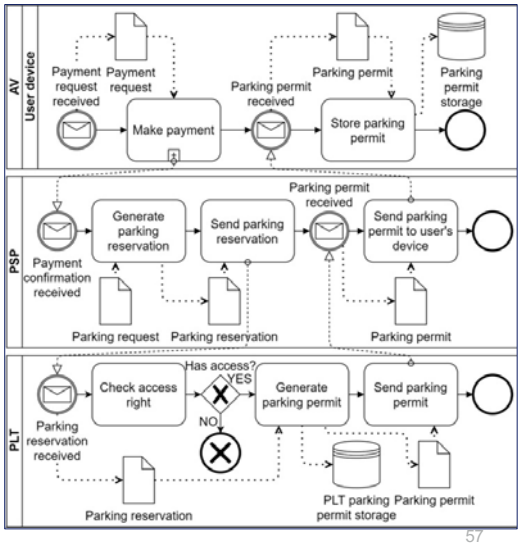
- *Security Risk Management*
- *Management of Personal Information*
- ***Management of Forensic Evidence***

RQ: How to manage forensic evidence?

UNIVERSITY OF TARTU
Institute of Computer Science

Vehicle Parking Scenario

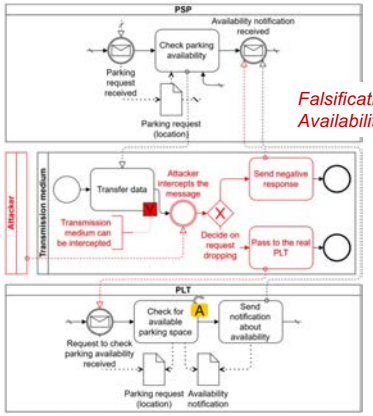
- Pre-payment
- Parking permit issue



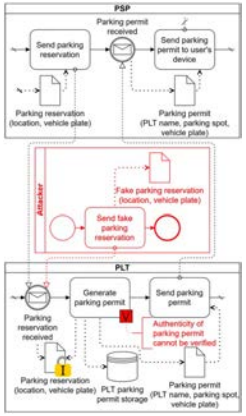
(Daubner et al. 2021)

UNIVERSITY OF TARTU
Institute of Computer Science

Security Risk Scenarios



Falsification of Availability Reports



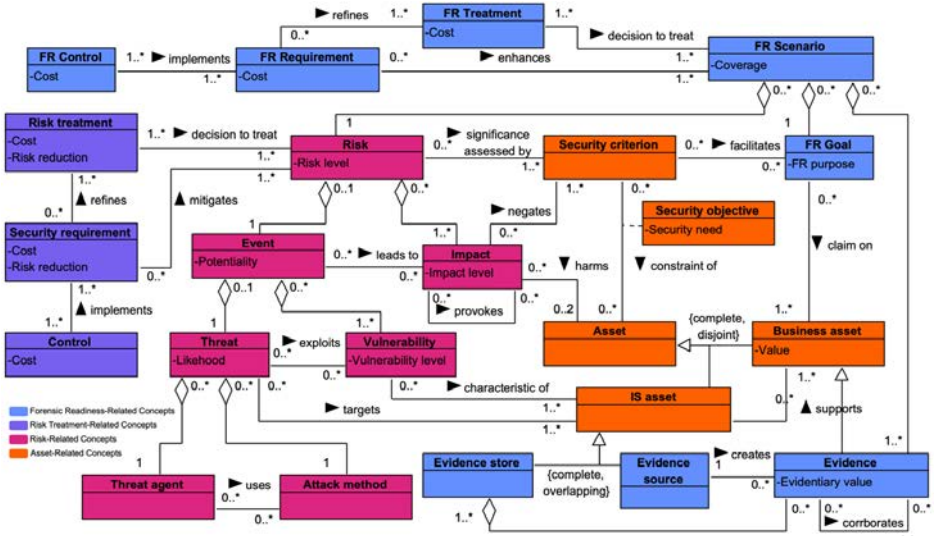
Fabrication of Parking Permit

(Daubner et al. 2022)

UNIVERSITY OF TARTU
Institute of Computer Science

Key concepts

Concept	[Tan, 2001]	[Rowlingson, 2004	[Grobler et al., 2010]	[Elyas et al., 2015	[GPG 18, 2015]	[ISO/ IEC, 2015]
Potential evidence	Incident data, Log	Potential evidence	Evidence	Potential digital evidence	Digital evidence	Potential digital evidence
Evidence source	Source of evidence	Source of potential evidence	X	X	Digital evidence source	Potential source of digital evidence
Evidence storage	Storage for Log Data	Secure Storage	X	X	X	X
Event	Incident	Incident, Criminal act	X	X	X	X
Impact	X	Impact	X	X	Impact, Harm	X
Risk	X	Risk	Risk	X	Risk	Risk
FR Scenario	X	Business scenario benefiting froom evidence	Incident	X	Scenario	Scenario
FR Goal	X	Benefit	X	Forensic, Readiness, Objective	Benefit, Scenario, Class	X
FR Treatment	X	X	X	X	X	X
FR Requirement	X	Evidence, Colllection, Requirement	Evidence Requirement	X	X	X
FR Control	X	Evidence, Gathering, Capability	X	Forensic Technology/ Architecture	X	Control



(Daubner et al. 2022)

Evidence View

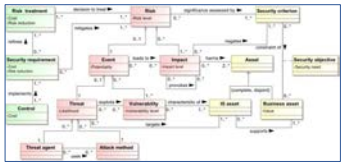
Nominal execution will contain everything
- Anomalous (an attack) should not

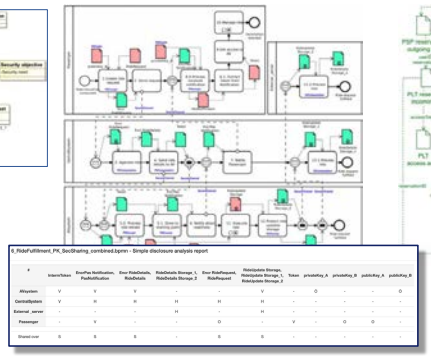
(Daubner et al. 2022)

Other Examples

Forensic ready system to capture **Insider Attacks**
- L Daubner, M Macak, R Matulevičius, B Buhnova, S Maksović, T Pitner (2023): Addressing insider attacks via forensic-ready risk management. Journal of Information Security and Applications 73, 103433

On Security of Intelligent Infrastructures





CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

chaise
blockchain skills for Europe
https://chaise-blockchainskills.eu/