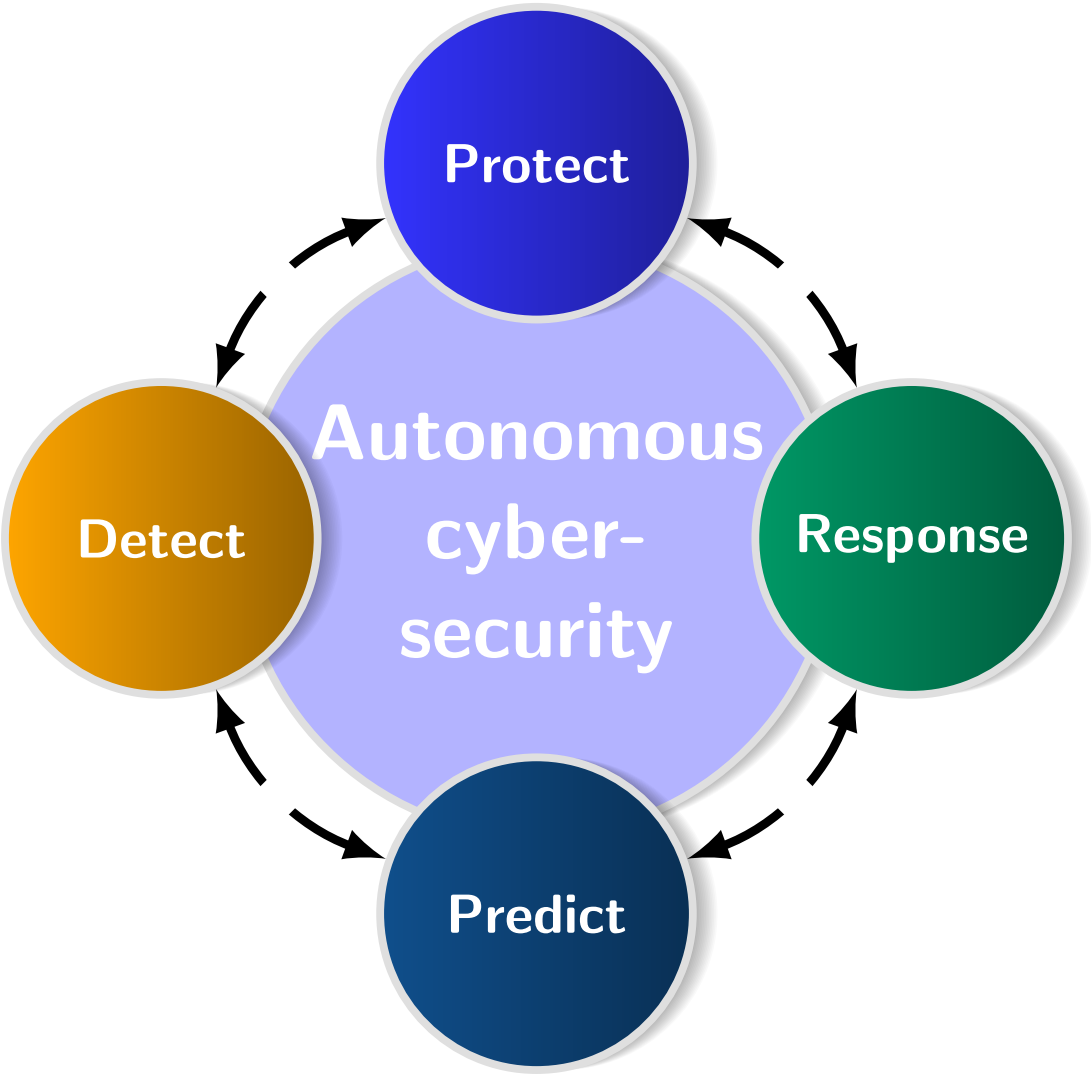
Cybersecurity through openness

David Arroyo

GICP

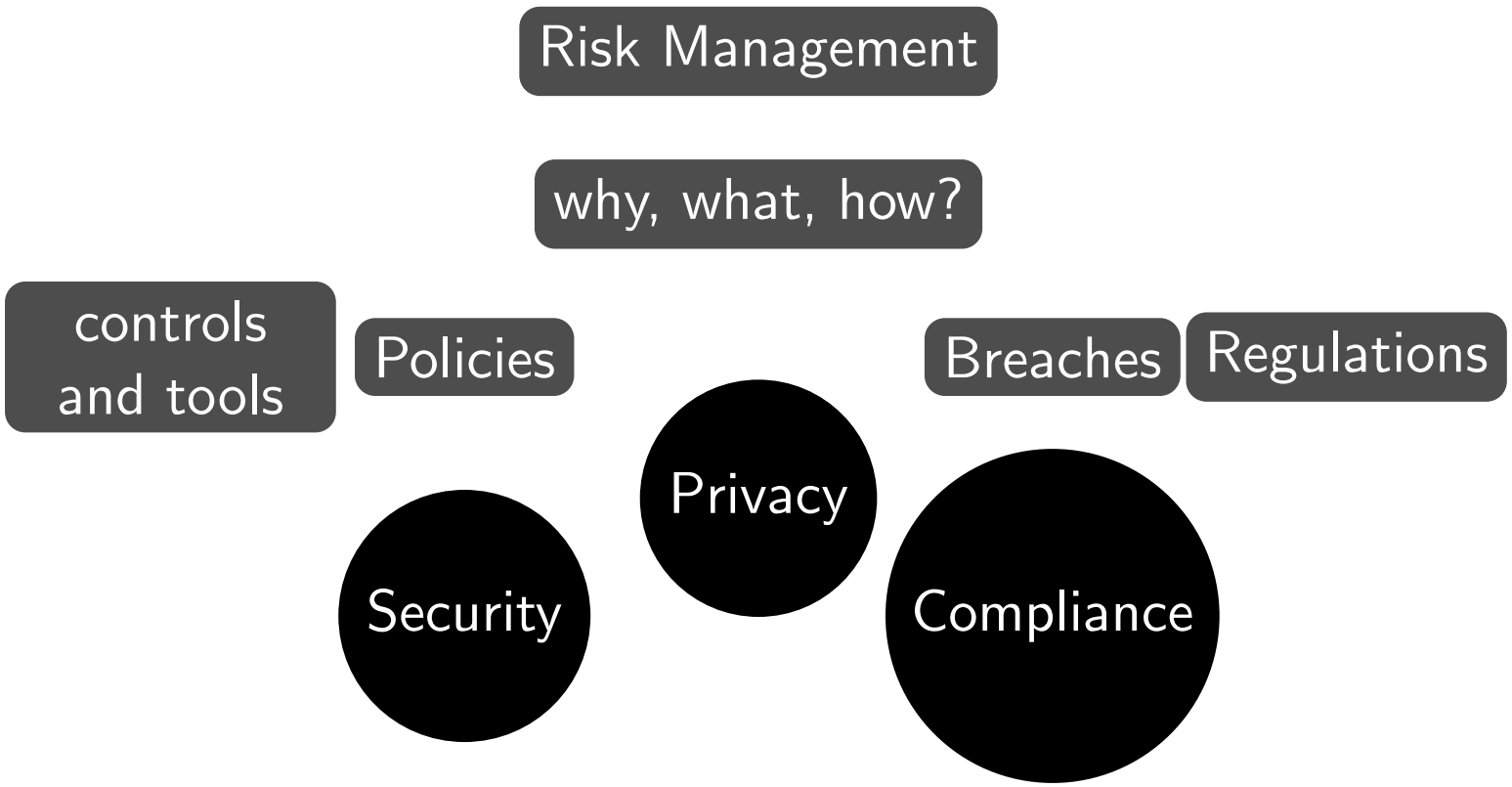

Protect
Detect
Autonomous cyber-security
Response
Predict

Funding

Grant Agreement No. 952622 under the EU H2020

Grant Agreement No. 101070660 under the EU HE

Grant Agreement No. 872855 under the EU H2020



[1]

[1] https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/privacy-preserving-analytics-and-secure-multiparty-computation

Main cybersecurity challenges I

- Systems obsolescence: bugs, vulnerabilities and outdated updates (hardware $\leftrightarrow$ firmware $\leftrightarrow$ software)

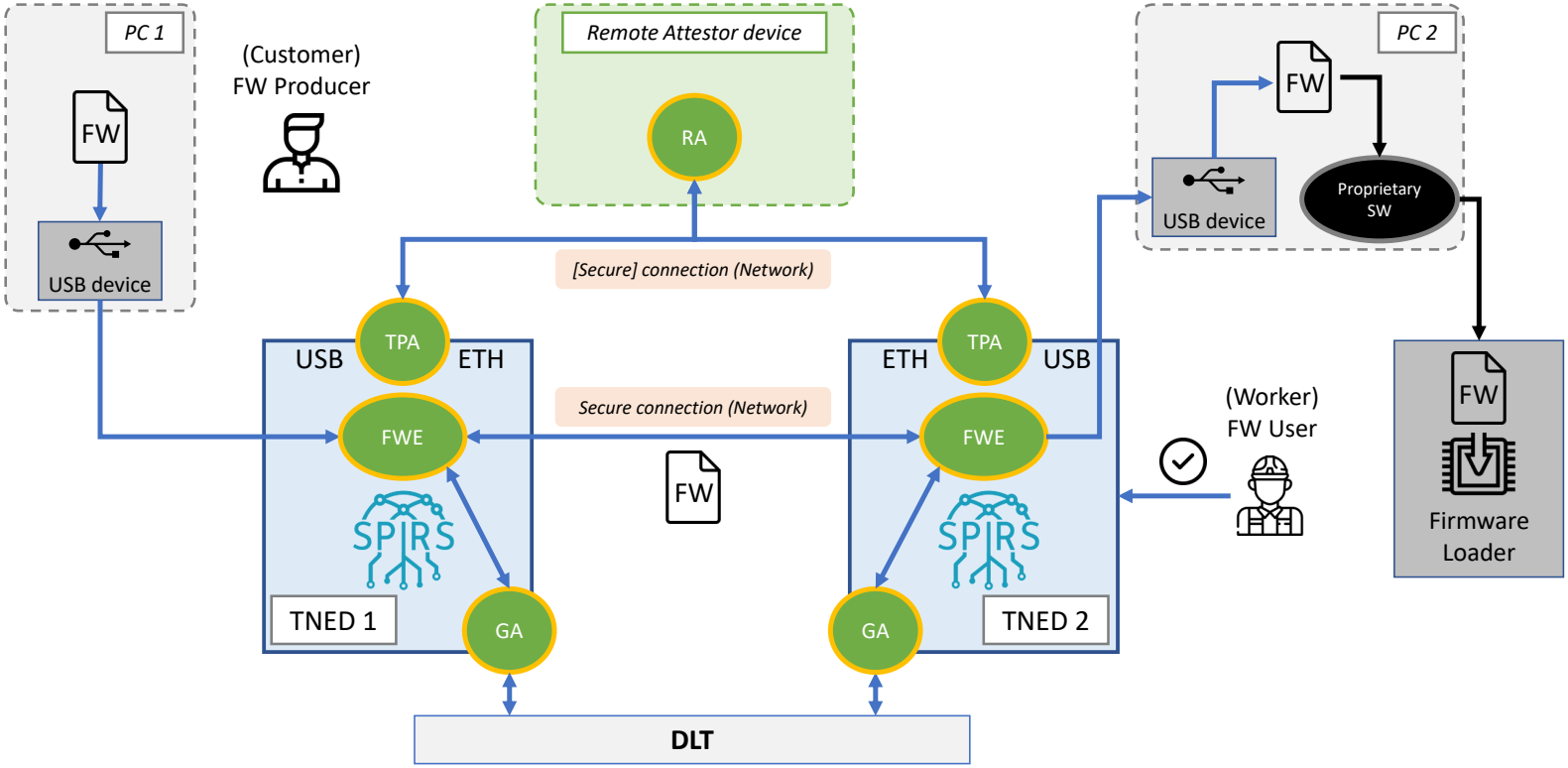
SE Radio 559: Ross Anderson on Software Obsolescence

Filed in Episodes by SE Radio on April 12, 2023 • 1 Comment

Ross John Anderson, Professor of Security Engineering at University of Cambridge, discusses software obsolescence with host Priyanka Raghavan. They examine risks associated with software going obsolete and consider several examples of software obsolescence, including how it can affect cars. Prof. Anderson discusses policy and research in the area of obsolescence and suggests some ways to mitigate the risks, with special emphasis on software bills of materials. He describes future directions, including software policy and laws in the EU, and offers advice for software maintainers to hedge against risks of obsolescence.

Main cybersecurity challenges II

- SPIRS use cases



- Insufficient cyber-awareness: ⇓ cyber-hygiene, responsible use of technology

Main cybersecurity challenges III

- avoid Luddite rejection but also technophilia uncritical acceptance Maria-Elena Osiceanu (2015). "Psychological Implications of Modern Technologies: "Technofobia" versus "Technophilia"". En: *Procedia - Social and Behavioral Sciences* 180. The 6th International Conference Edu World 2014 "Education Facing Contemporary World Issues", 7th - 9th November 2014, págs. 1137-1144. ISSN: 1877-0428
- Science Communication: Communicating Trustworthy Information in the Digital World

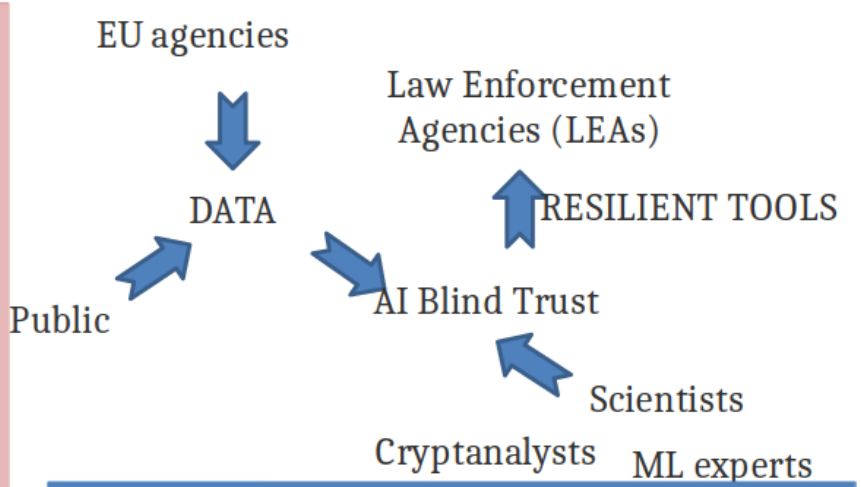
- (cyber)attacks sophistication: cyber-phyiscal domain
  - Atif Ahmad y col. (2019). "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack". En: *Computers & Security* 86, págs. 402-418

Coherent framework for the creation/management of high-quality training/testing data sets for AI

GICP

Data curation and health

- High-quality training and testing data sets for AI and needed technical developments
- Data minimization and trust management for cyberintelligence sharing
- Confidentiality and privacy protection by default
- Standards for IT and AI governance

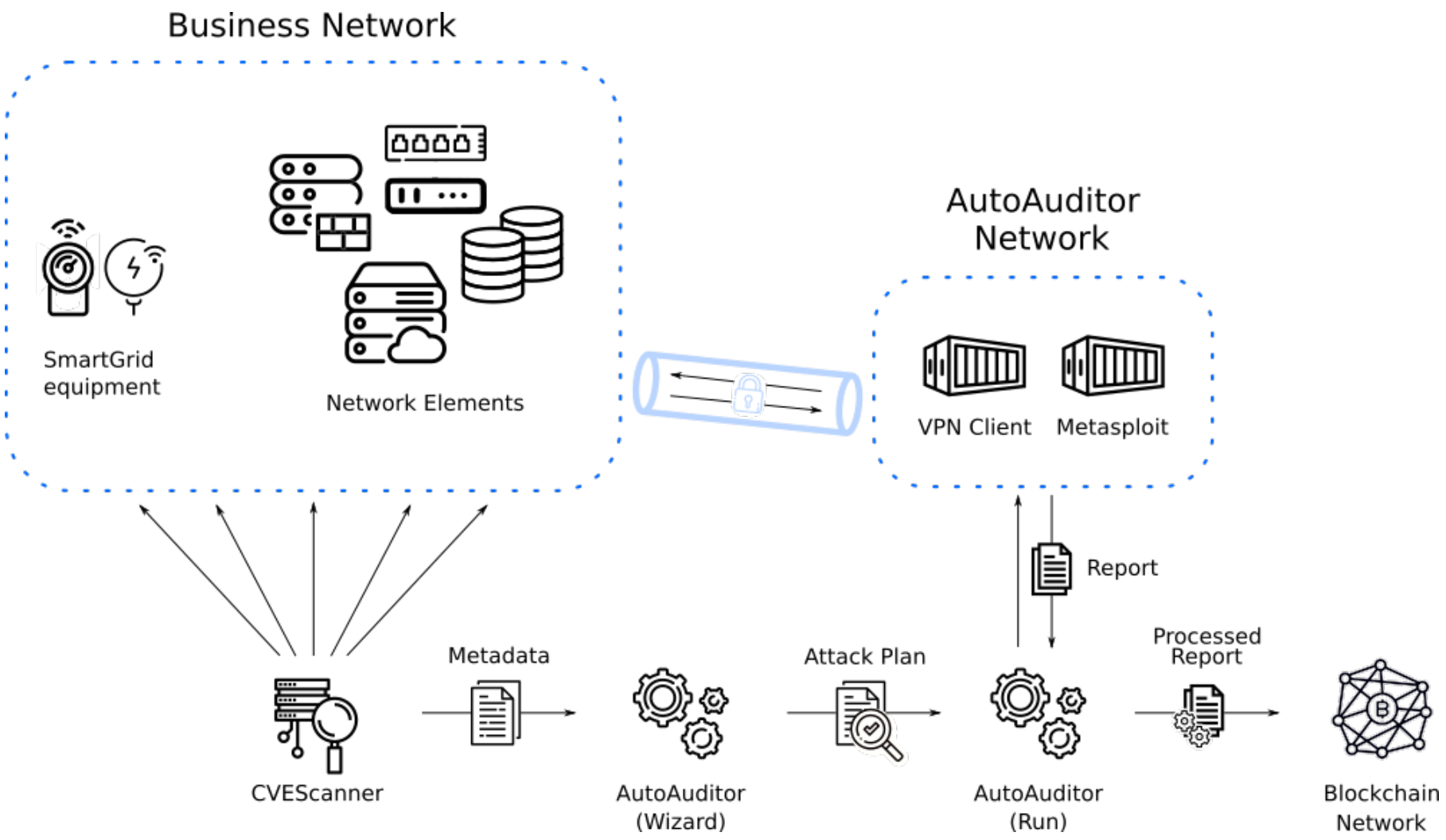


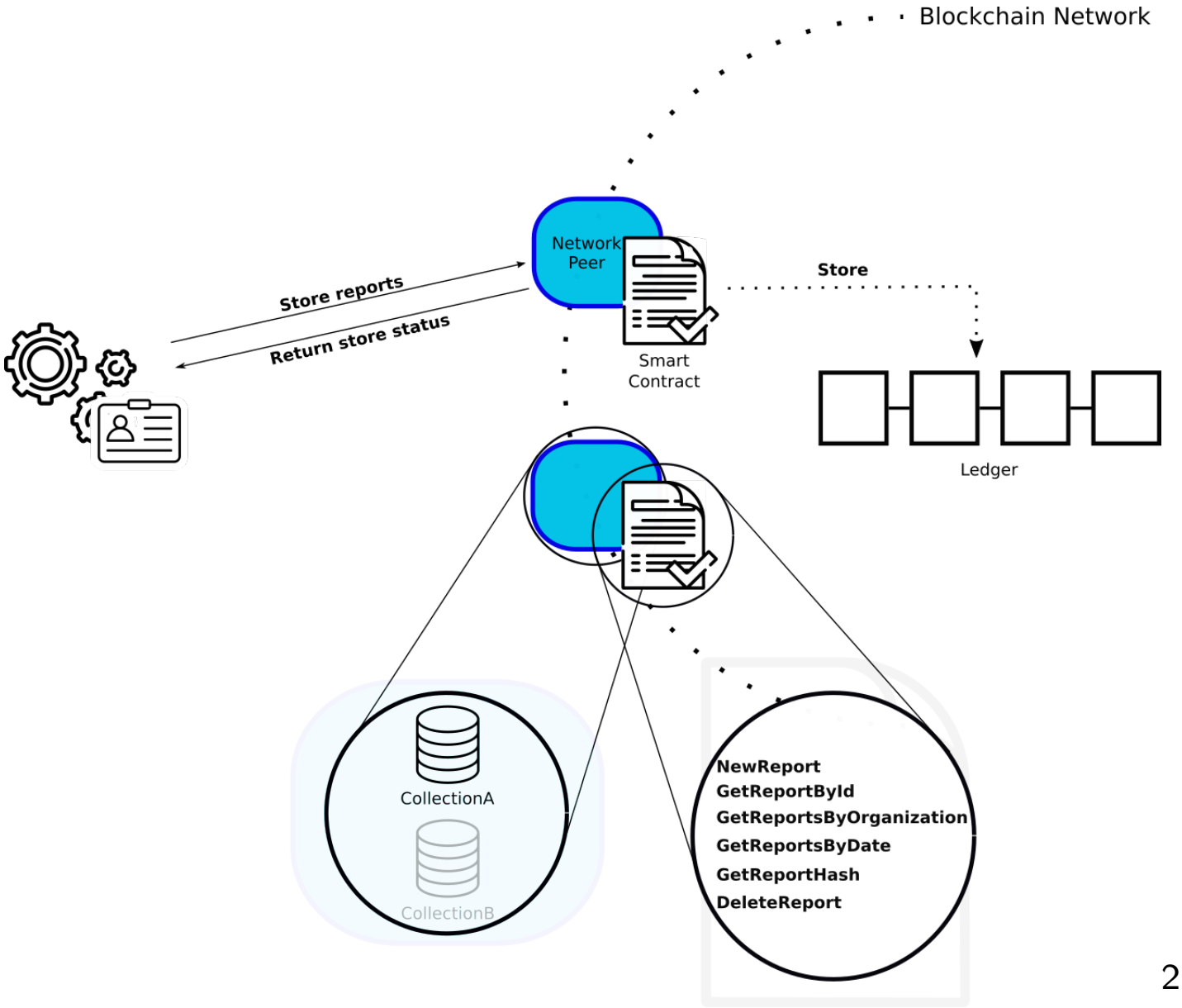
Multidisciplinary point of view

- ICT and cryptographic engineering
- socio-economic science and humanities
- gender studies

- Development of cyber-awareness campaigns to foster a better understanding and public acceptance of AI tools for law enforcement
- Comparative analysis of existing EU national legal provisions enabling the sharing of LEA and judiciary systems data
- Legislative changes at European and Member State level
- Ethical and operational implications for LEAs

Andrés Marın-López y col. (2020). “Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain”. En: *Electronics* 9.11, pág. 1865


Business Network
SmartGrid equipment
Network Elements
AutoAuditor Network
VPN Client
Metasploit
Report
Metadata
Attack Plan
Processed Report
CVEScanner
AutoAuditor (Wizard)
AutoAuditor (Run)
Blockchain Network



[2]

[2] https://gitlab.gast.it.uc3m.es/schica/autoauditor

Sergio Chica y col. (2023). "Enhancing the anonymity and auditability of whistleblowers protection". En: *Blockchain and Applications, 4th International Congress*. Springer, págs. 413-422

The European Commission decides to refer 8 Member States to the Court of Justice of the European Union over the protection of whistleblowers

Page contents

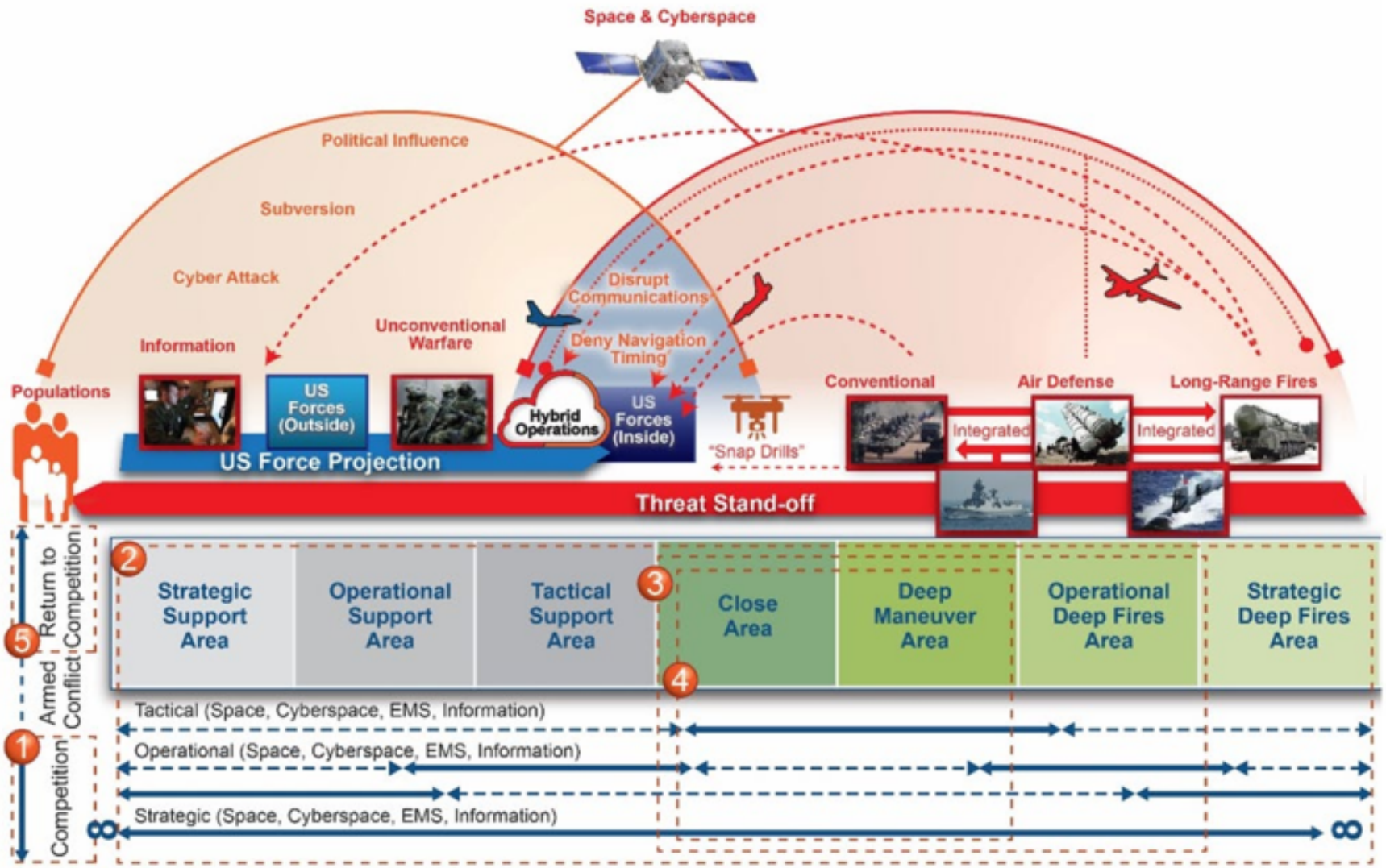
- Top
- Print friendly pdf
- Contacts for media

Today, the European Commission decided to refer **Czechia, Germany, Estonia, Spain, Italy, Luxembourg, Hungary and Poland** to the Court of Justice for failure to transpose and notify the national measures transposing the directive on the protection of persons who report breaches of Union law into their legal framework (Directive (EU) 2019/1937).

https://www.diana.nato.int/challenges.html

creating a secure and trusted information environment – with the emphasis on live data streams such as those used to provide near real-time video, augmented reality feeds, digital radio and more. Of particular interest are hardware and software solutions that operate over open networks and that can function in 'austere' or 'disadvantaged' environments

Multi-domain operations[3]



[3] TRADOC, 'TRADOC Pamphlet 525-3-8 – U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045', December 2018

Sara Degli Esposti y Carles Sierra (2021). *White Paper on Artificial Intelligence, Robotics and Data Science*. Consejo Superior de Investigaciones Cientificas (España)


CHALLENGE 8

SMART CYBERSECURITY

Coordinators

D. Arroyo Guardeño (ITEFI, CSIC)

P. Reon Jiménez (IMAT-CSIC, CSIC - US)

Participant researchers and centers

J. Godoy (CAR, CSIC - UPM)

J. Villagra (CAR, CSIC - UPM)

H. Mueller (IAE, CSIC)

V. Gallego (ICMAT, CSIC-UAM-UC3M-UCM)

A. Kozgodagan (ICMAT, CSIC-UAM-UC3M-UCM)

R. Navarro (ICMAT, CSIC-UAM-UC3M-UCM)

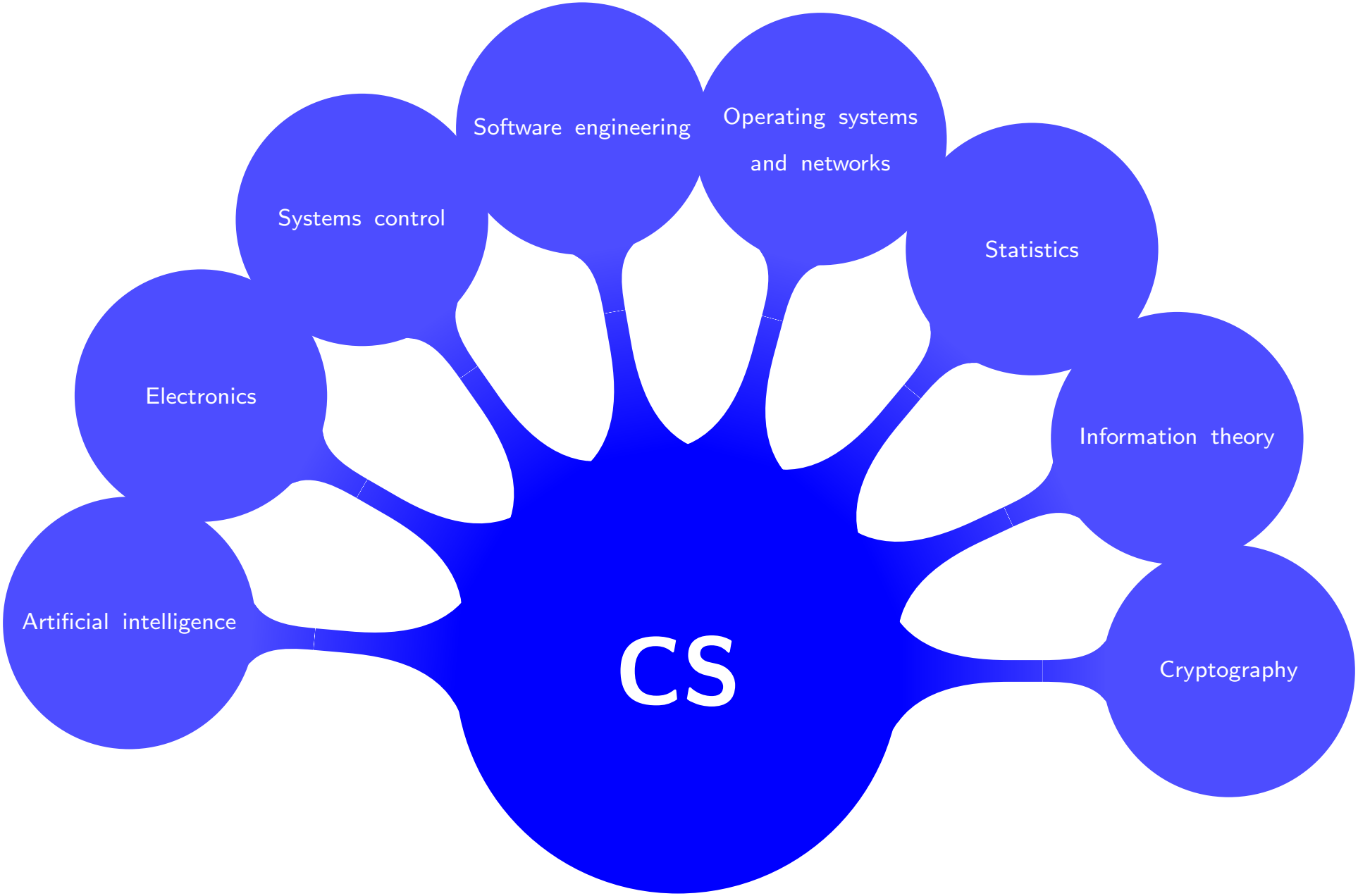
D. Blico Irazoa (ICMAT, CSIC-UAM-UC3M-UCM)

D. Rodríguez González (IFCA, CSIC - UC)

S. Hidalgo Villena (IMB-CSIC)

S. Degli Esposti (IPP, CSIC)

P. Noheda Marín (IQOG, CSIC)


Software engineering
Operating systems and networks
Systems control
Statistics
Electronics
Information theory
Artificial intelligence
CS
Cryptography

Smart cybersecurity: key challenging points

1. Fighting Misinformation About Science
2. Imposing Security-by-Default Along the Computing System by Leveraging AI
3. Creating a Formal Model for Adversarial Machine Learning
4. Safeguarding Privacy in the Era of Big Data and AI

Smart cybersecurity: key challenging points

1. Fighting Misinformation About Science

   EDMO
   European Digital Media Observatory

2. Imposing Security-by-Default Along the Computing System by Leveraging AI
3. Creating a Formal Model for Adversarial Machine Learning
4. Safeguarding Privacy in the Era of Big Data and AI

Smart cybersecurity: key challenging points

1. Fighting Misinformation About Science
2. Imposing Security-by-Default Along the Computing System by Leveraging AI

3. Creating a Formal Model for Adversarial Machine Learning
4. Safeguarding Privacy in the Era of Big Data and AI

Smart cybersecurity: key challenging points

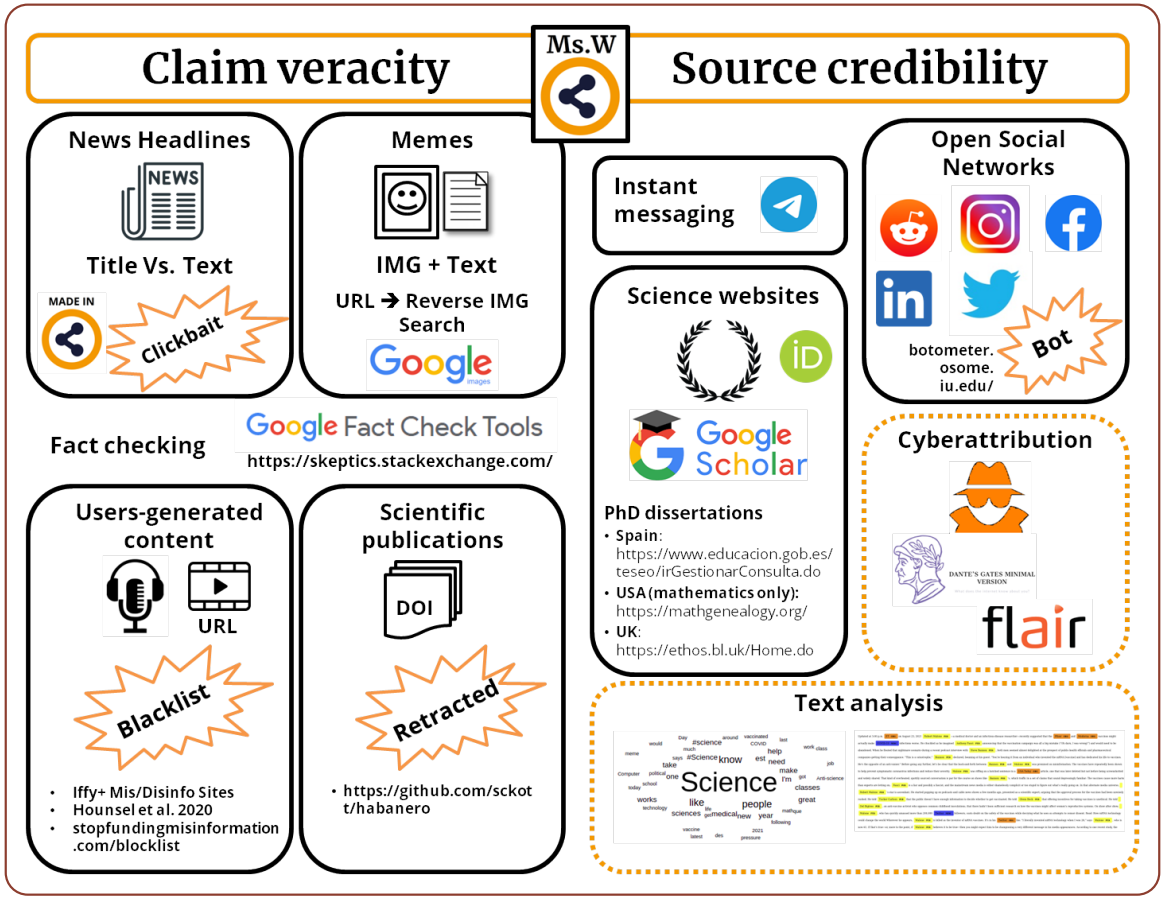
1. Fighting Misinformation About Science
2. Imposing Security-by-Default Along the Computing System by Leveraging AI
3. Creating a Formal Model for Adversarial Machine Learning

4. Safeguarding Privacy in the Era of Big Data and AI

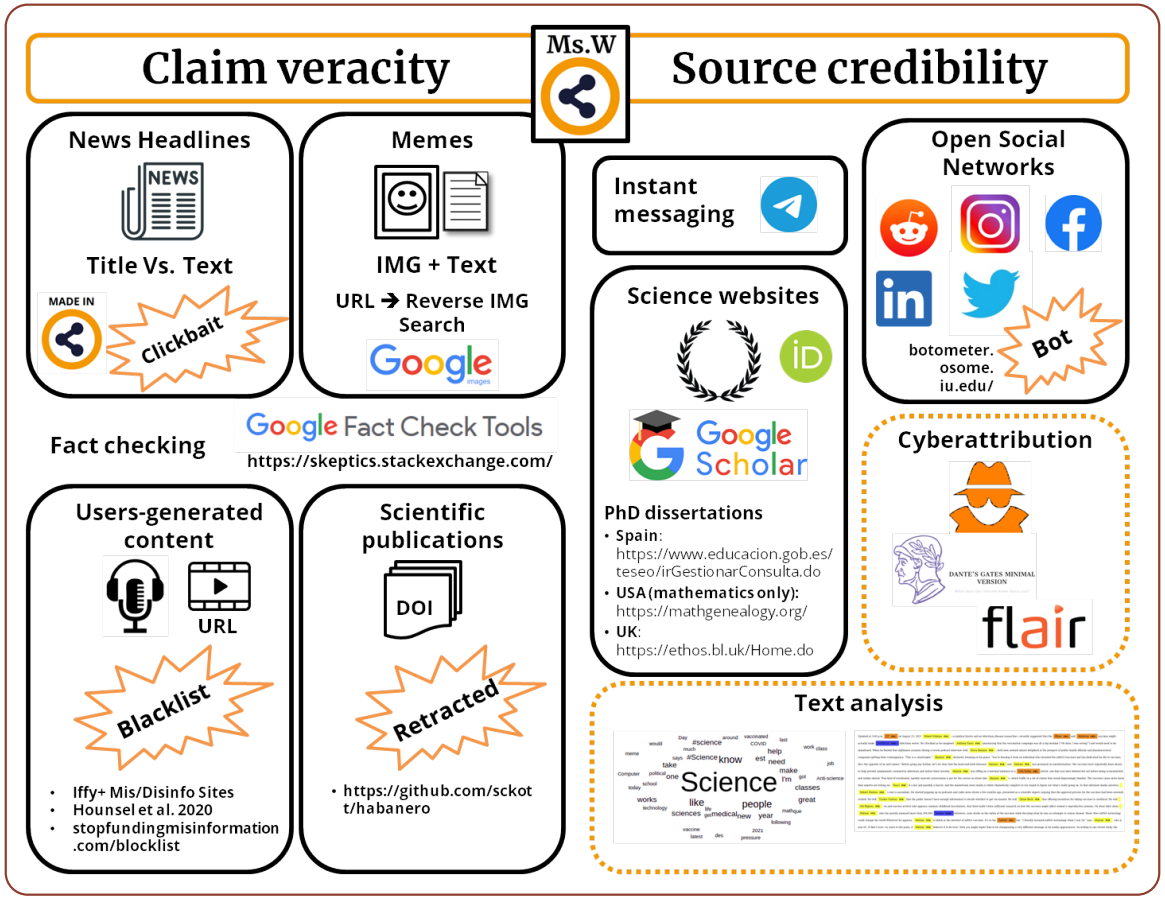
Smart cybersecurity: key challenging points

1. Fighting Misinformation About Science
2. Imposing Security-by-Default Along the Computing System by Leveraging AI
3. Creating a Formal Model for Adversarial Machine Learning
4. Safeguarding Privacy in the Era of Big Data and AI

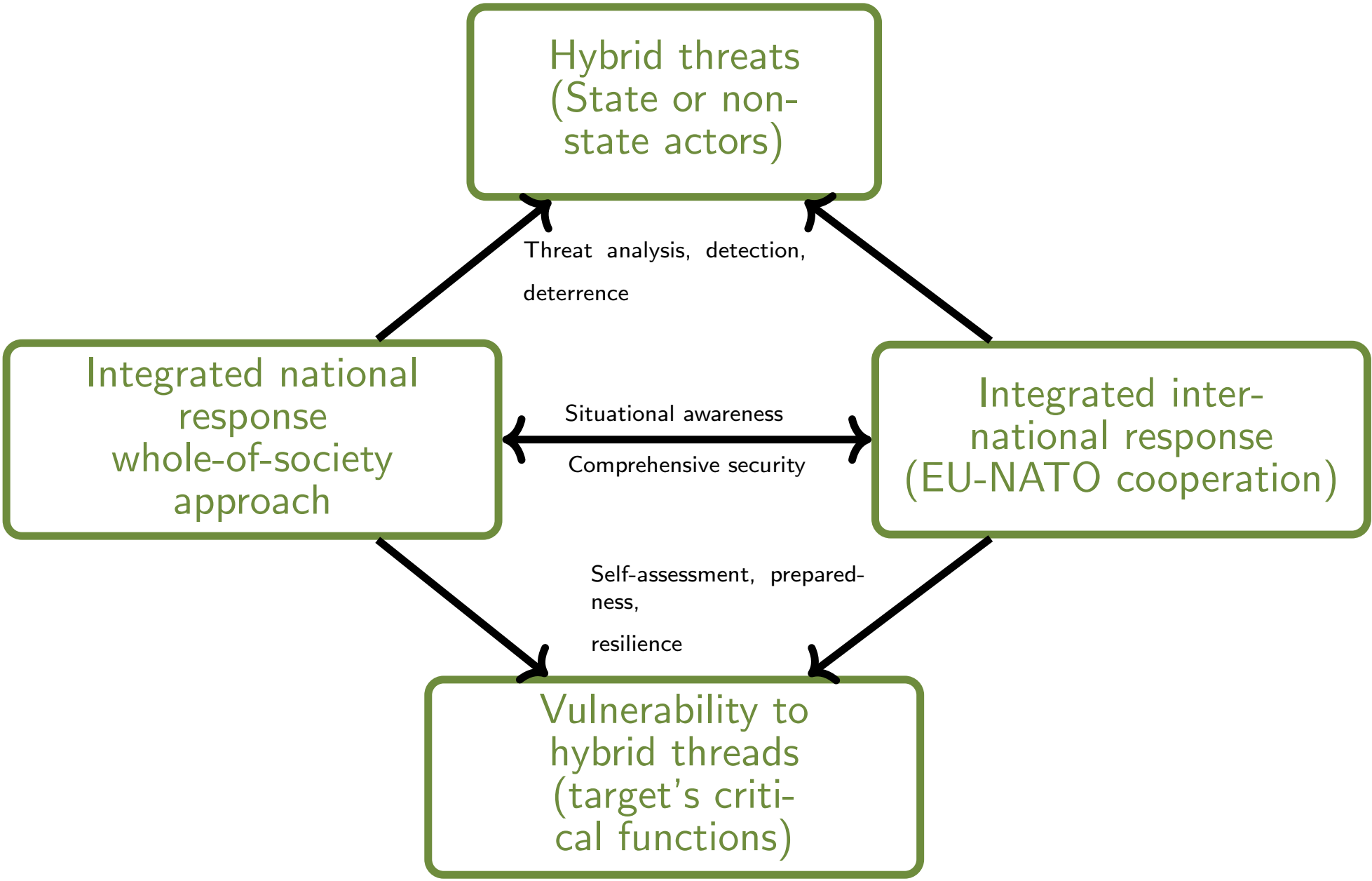
Trust in the trustworthy



Trust in the trustworthy



An interdisciplinary view of the role of control, accountability, and digital surveillance in building trust relationships


Hybrid threats (State or non-state actors)
Threat analysis, detection, deterrence
Integrated national response whole-of-society approach
Situational awareness
Comprehensive security
Integrated international response (EU-NATO cooperation)
Self-assessment, preparedness, resilience
Vulnerability to hybrid threads (target's critical functions)

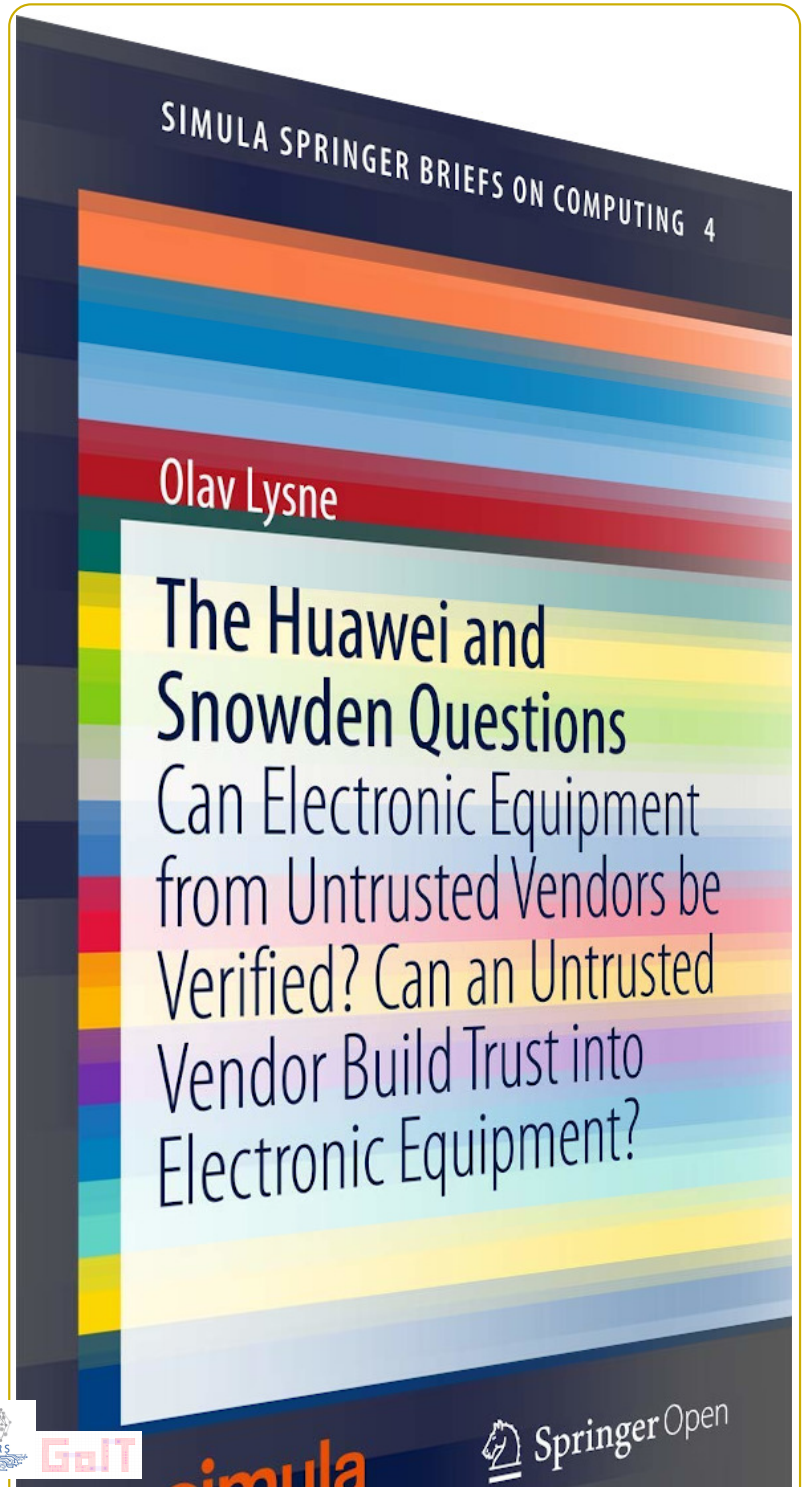
SU-ICT-02-2020-Building blocks for resilience in evolving ICT systems

SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS

Acronym: SPIRS

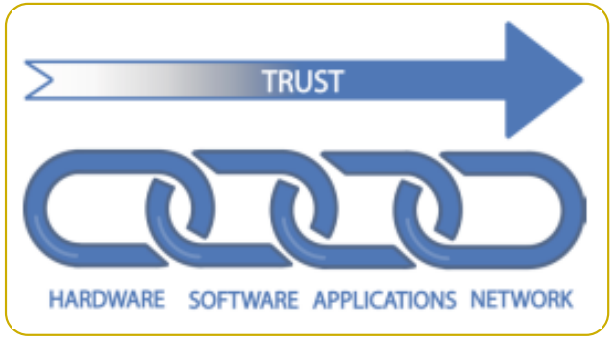
List of participants

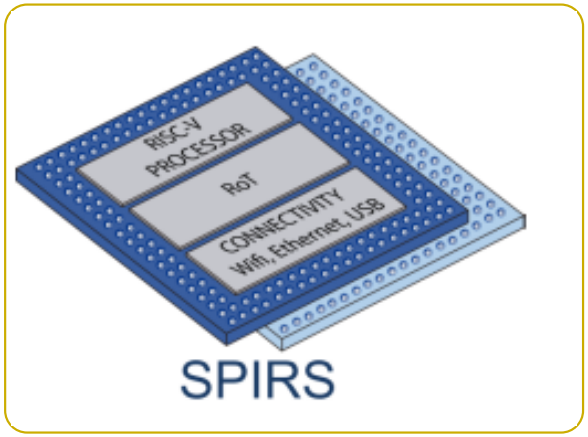
Participant No. *	Participant organisation name	Country
1 (Coordinator)	Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC)	Spain
2	Tampere University (TAU)	Finland
3	Politecnico di Torino (POLITO)	Italy
4	Telefónica Investigación y Desarrollo SA (TID)	Spain
5	Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	France
6	Fondazione LINKS – Leading Innovation & Knowledge for Society (LINKS)	Italy
7	Next SRL (NEXT)	Italy
8	NEC Laboratories Europe GmbH (NEC)	Germany
9	Thales DIS Design Services SAS (THALES)	France

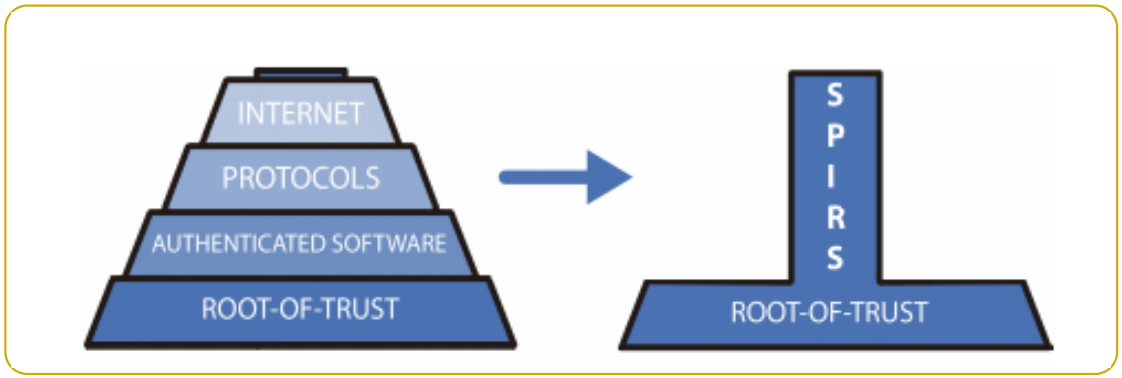


European Processor Initiative

Industrial Alliance for Processors and Semiconductor Technologies







The danger of supply-chain attacks I

Mark Beaumont y col. (2011). "Hardware Trojans-prevention, detection, countermeasu-
res". En: *DSTO, defense science and technology organization, PO Box* 1500

The danger of supply-chain attacks II

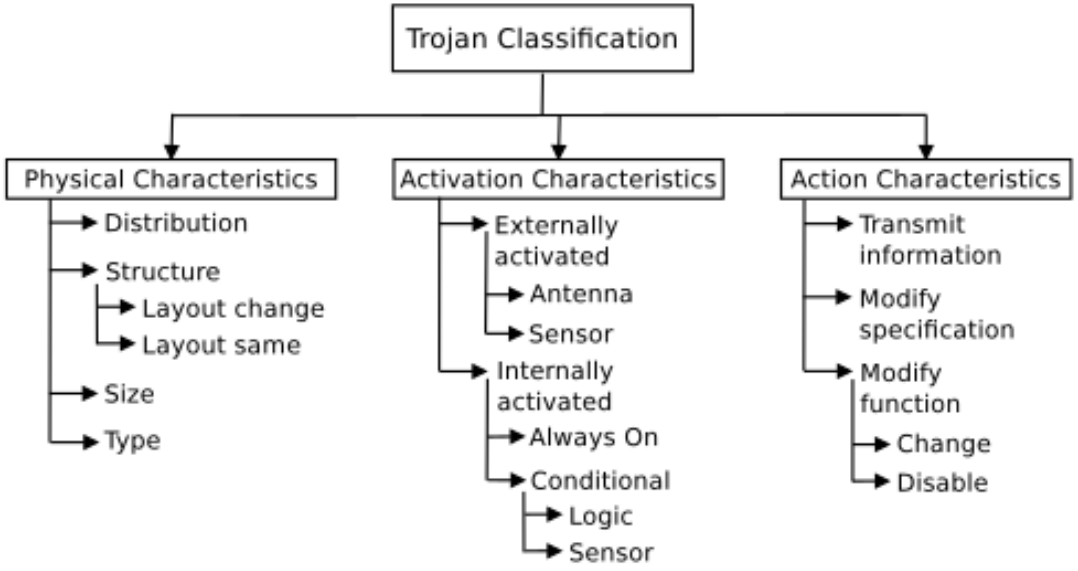
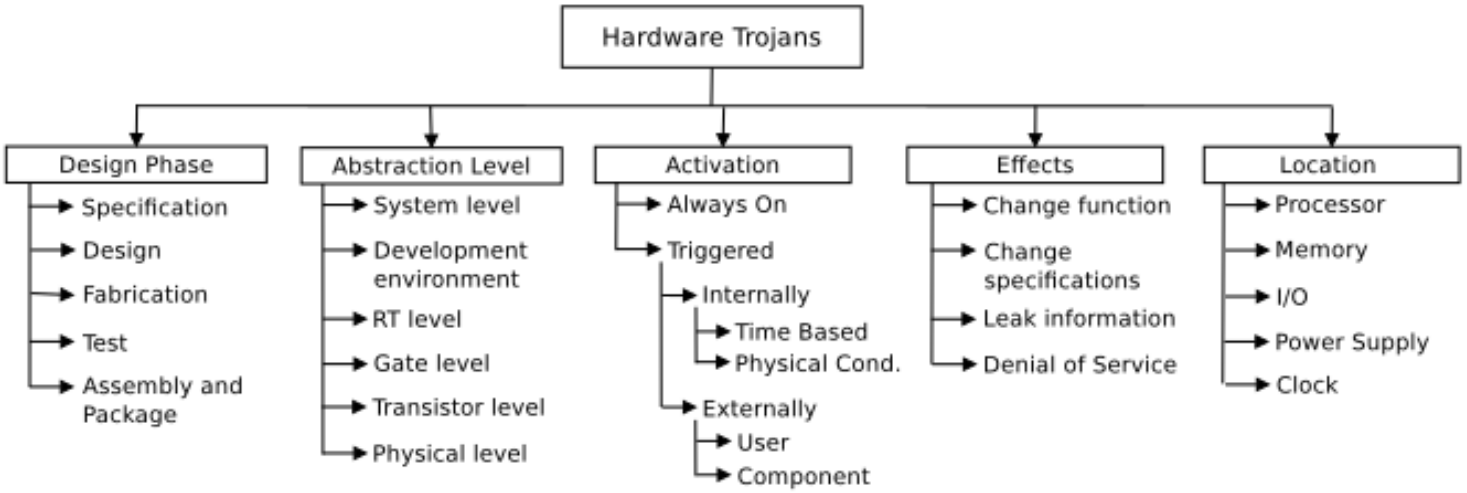
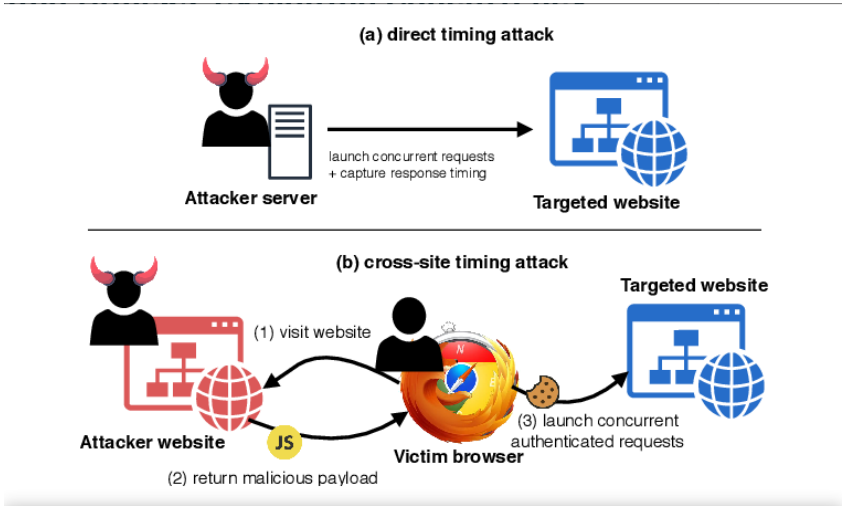


Figure 2: Hardware Trojan Taxonomy: Wang, Tehranipoor & Plusquellic (2008)



Comprehensive (BLT) Security solutions, otherwi

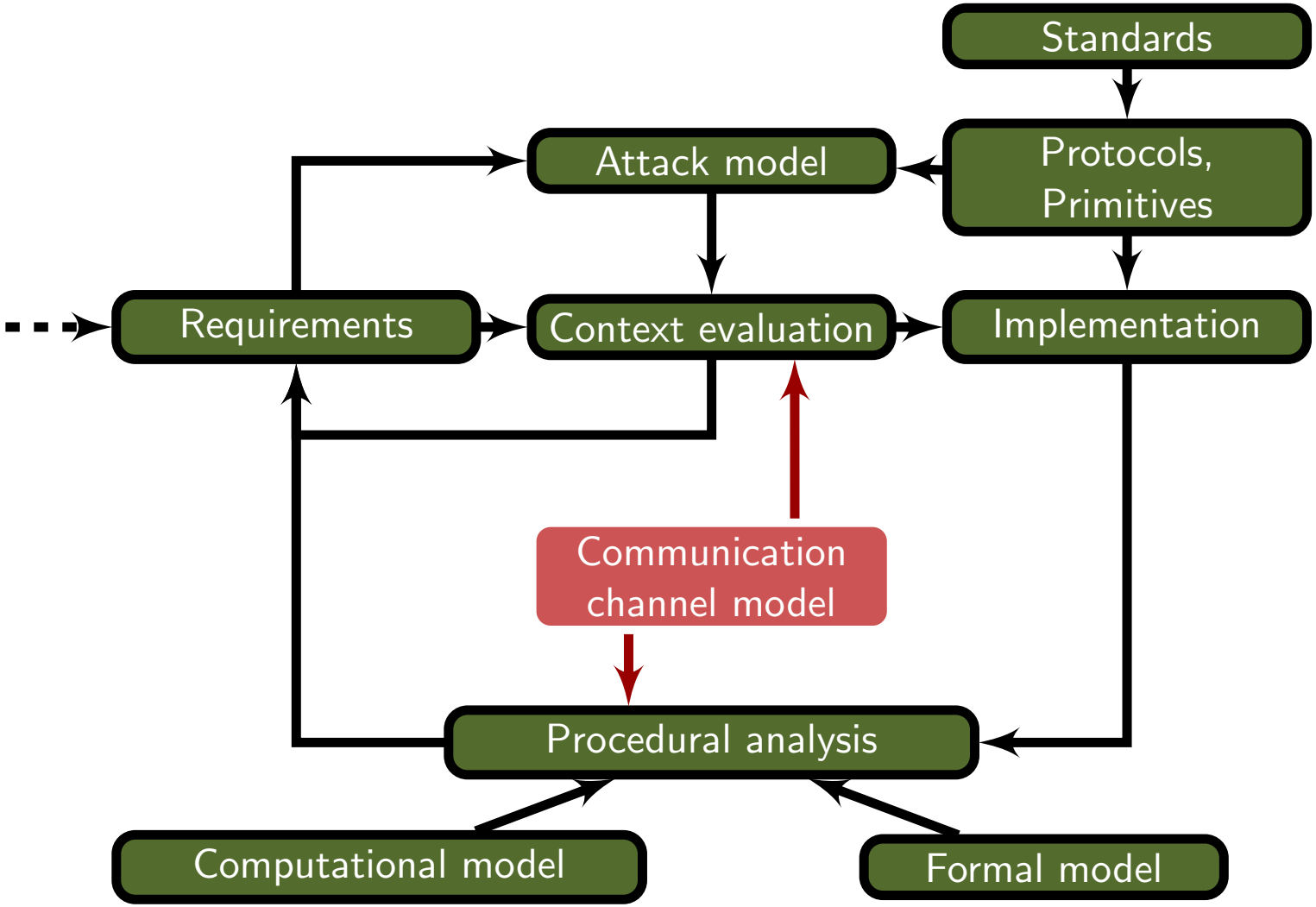
- have i been pwned? Check if you have an account that has been compromised in a data breach
- 'Worse Than KRACK' – Google And Microsoft Hit By Massive 5-Year-Old Encryption Hole
- Vietnamese researcher shows iPhone X face ID 'hack'
- Side channel attacks

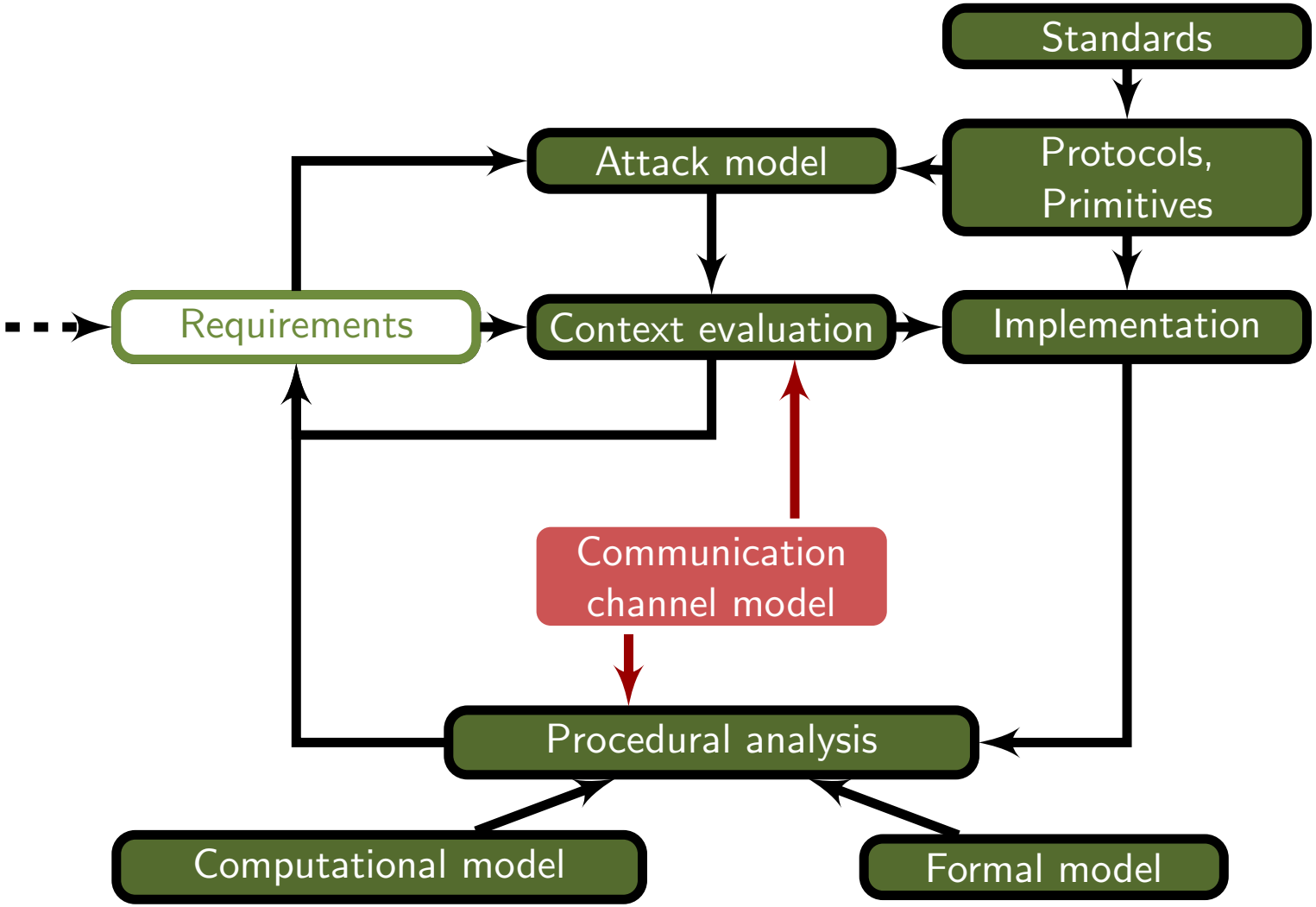


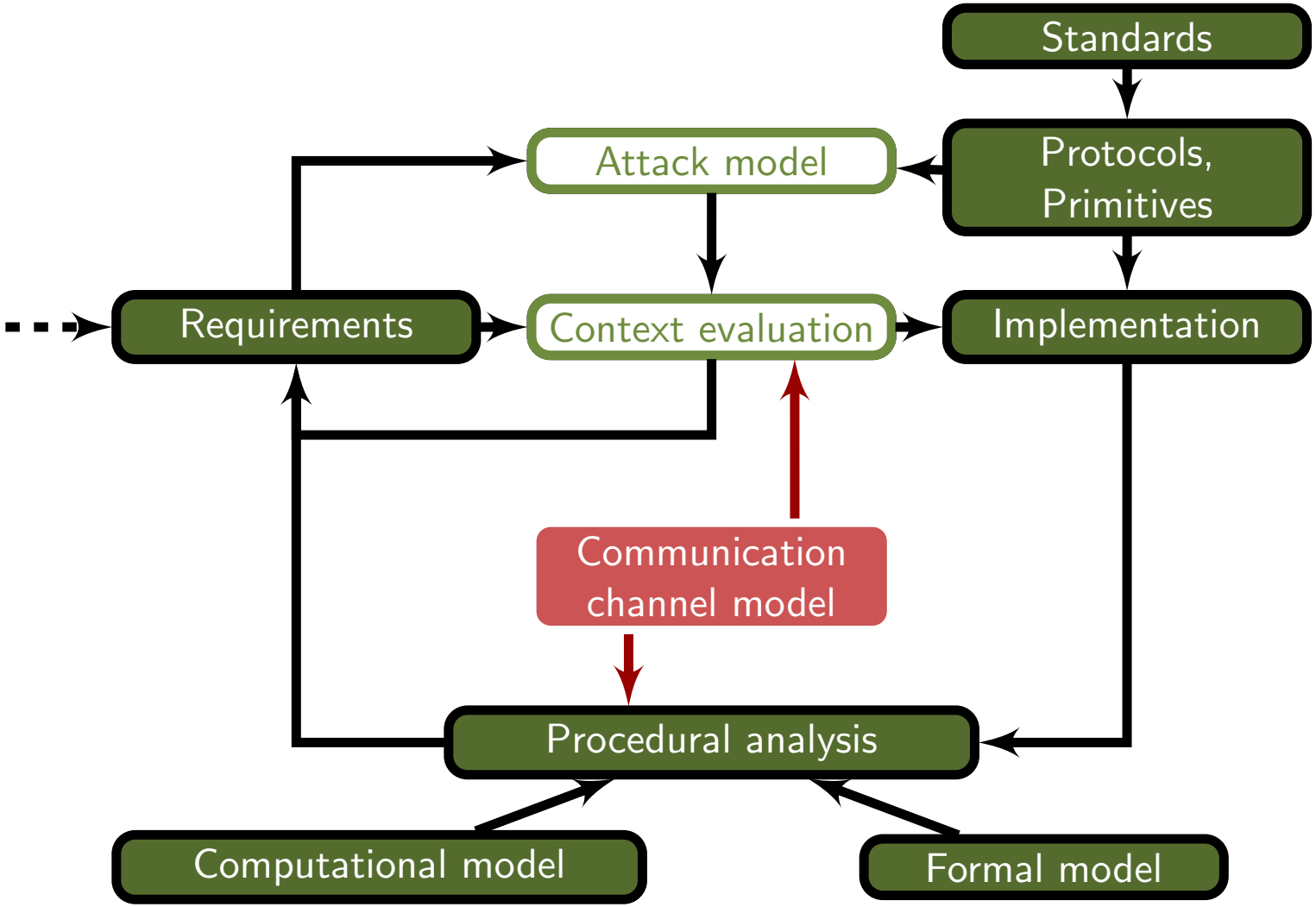
Tom Van Goethem y col. (2020). "Timeless timing attacks: Exploiting concurrency to leak secrets over remote connections". En: *29th {USENIX} Security Symposium ({USENIX} Security 20)*, págs. 1985-2002

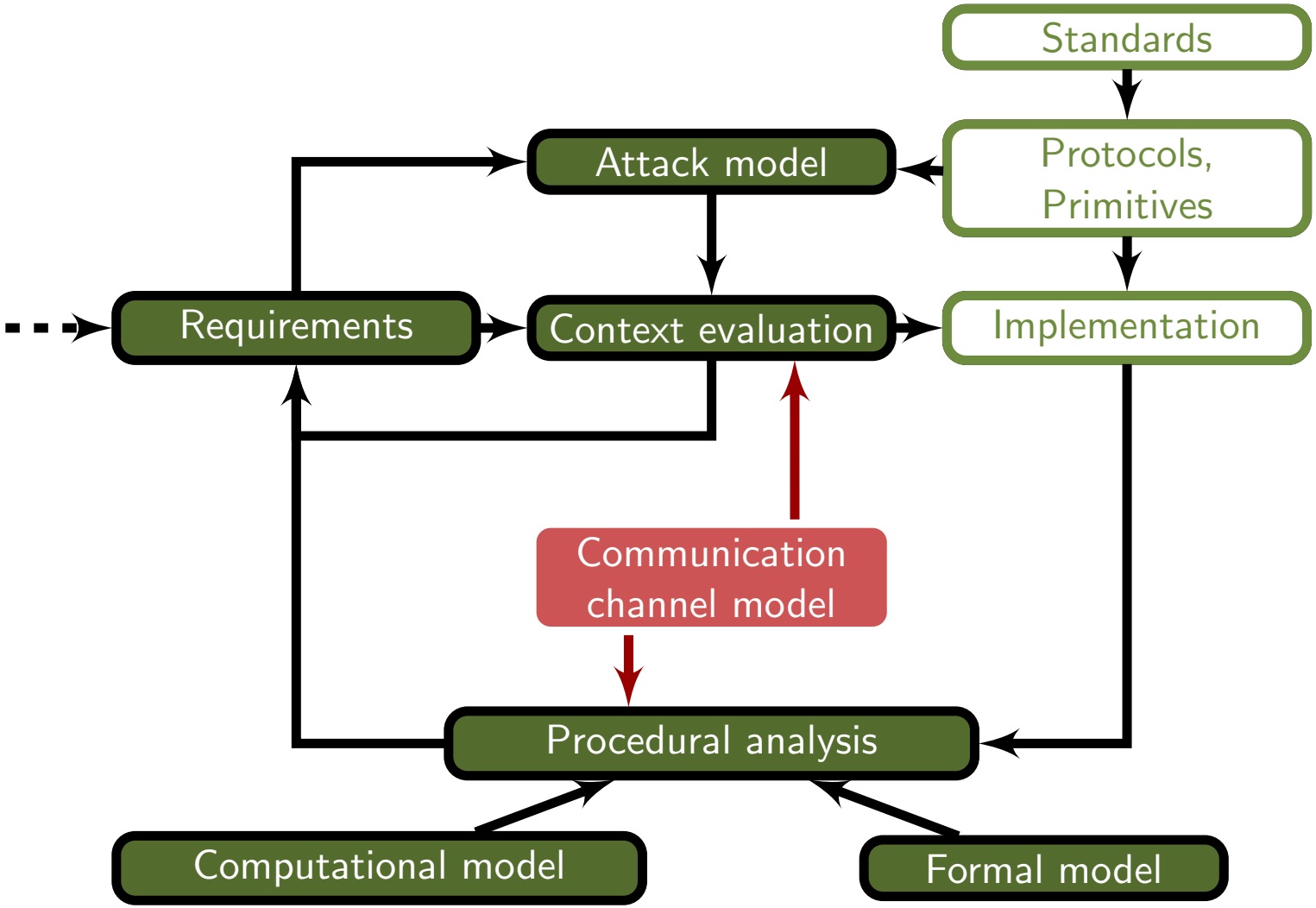
Comprehensive (BLT) Security solutions, otherwi

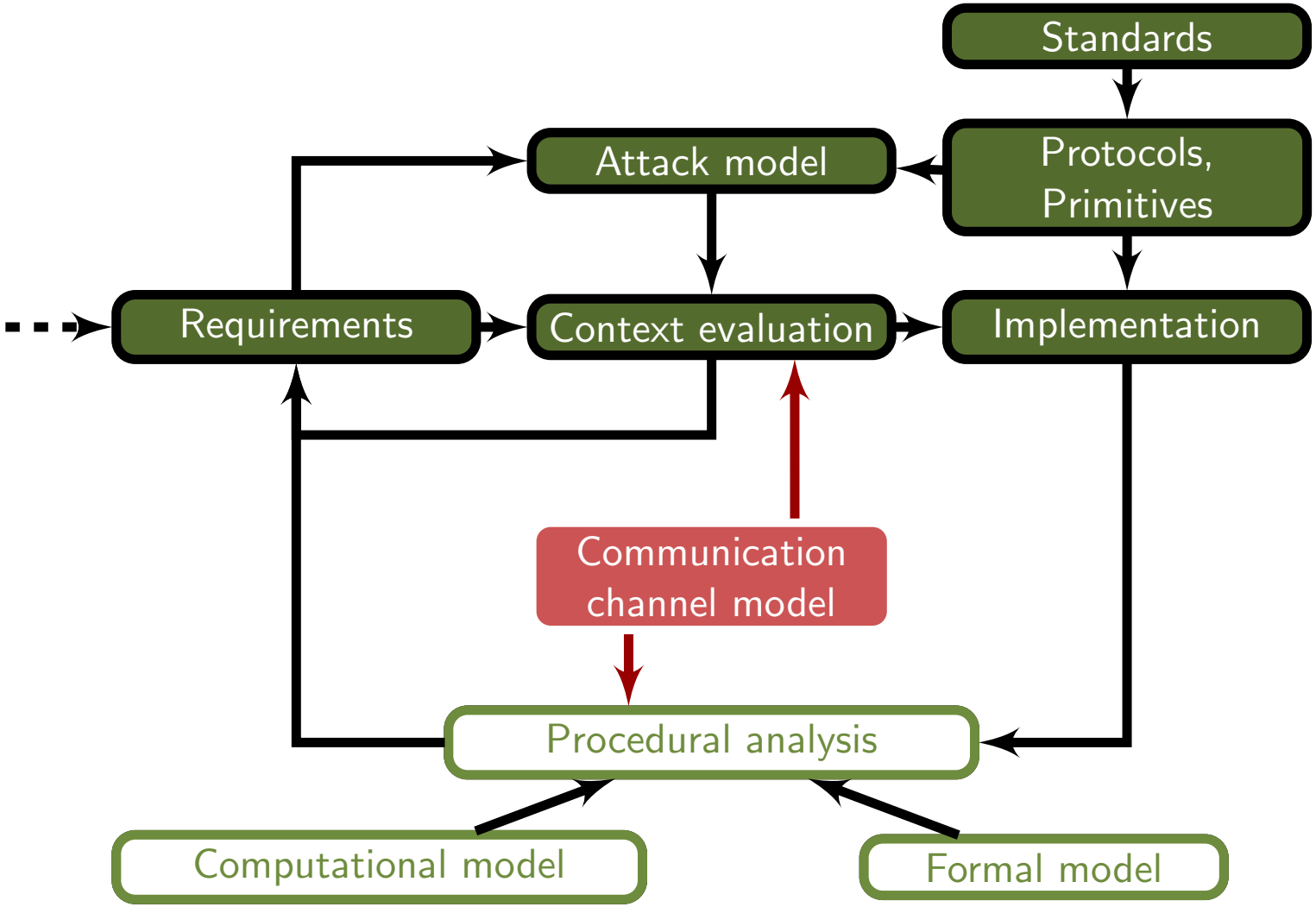
CALL FOR A PROPER Business, Law, and Technology approach

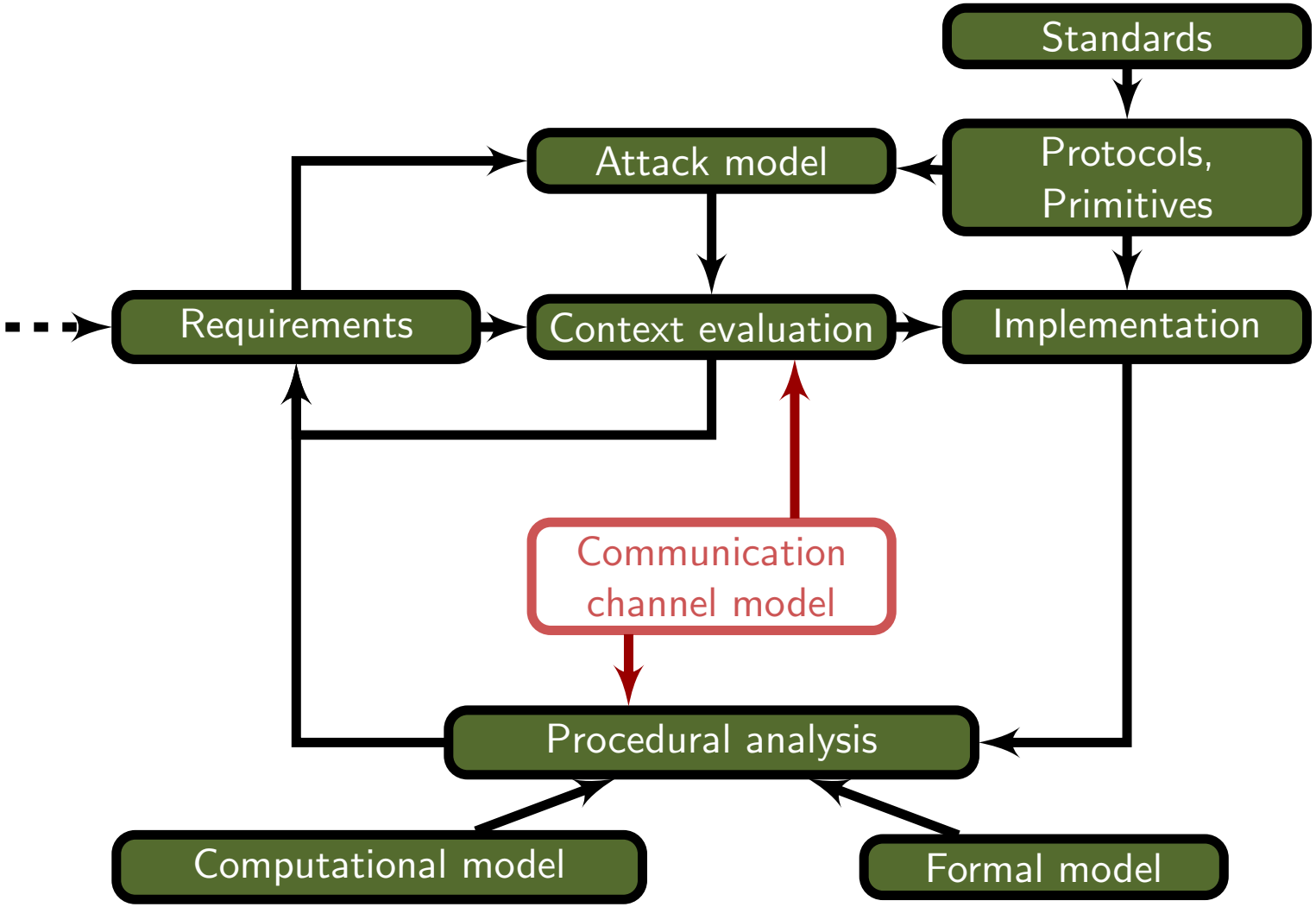

Standards
Attack model
Protocols, Primitives
Requirements
Context evaluation
Implementation
Communication channel model
Procedural analysis
Computational model
Formal model


Standards
Attack model
Protocols, Primitives
Requirements
Context evaluation
Implementation
Communication channel model
Procedural analysis
Computational model
Formal model


Standards
Attack model
Protocols, Primitives
Requirements
Context evaluation
Implementation
Communication channel model
Procedural analysis
Computational model
Formal model


Standards
Attack model
Protocols,
Primitives
Requirements
Context evaluation
Implementation
Communication
channel model
Procedural analysis
Computational model
Formal model


Standards
Attack model
Protocols, Primitives
Requirements
Context evaluation
Implementation
Communication channel model
Procedural analysis
Computational model
Formal model


Standards
Attack model
Protocols, Primitives
Requirements
Context evaluation
Implementation
Communication channel model
Procedural analysis
Computational model
Formal model


1234 5
9012 345G
CARDH ER 6/15
NAME


1234 5
9012 345G
CARDH ER 6/15
NAME


1234 5
9012 345G
CARDH ER G/15
NAME

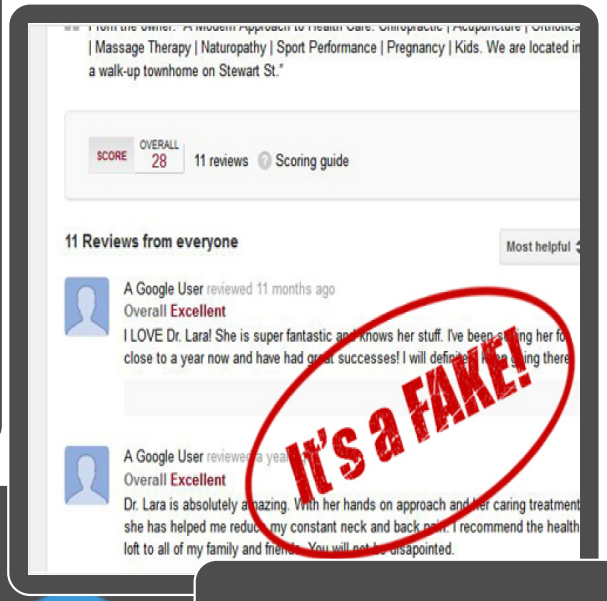

SPAM


| Massage Therapy | Naturopathy | Sport Performance | Pregnancy | Kids. We are located in
a walk-up townhome on Stewart St."
SCORE
OVERALL
28
11 reviews
Scoring guide
11 Reviews from everyone
Most helpful
A Google User reviewed 11 months ago
Overall Excellent
I LOVE Dr. Lara! She is super fantastic and knows her stuff. I've been seeing her for
close to a year now and have had great successes! I will definitely keep going there
A Google User
Overall Excellent
Dr. Lara is absolutely amazing. With her hands on approach and her caring treatment
she has helped me reduce my constant neck and back pain. I recommend the health
loft to all of my family and friends. You will not be disapointed.
It's a FAKE!

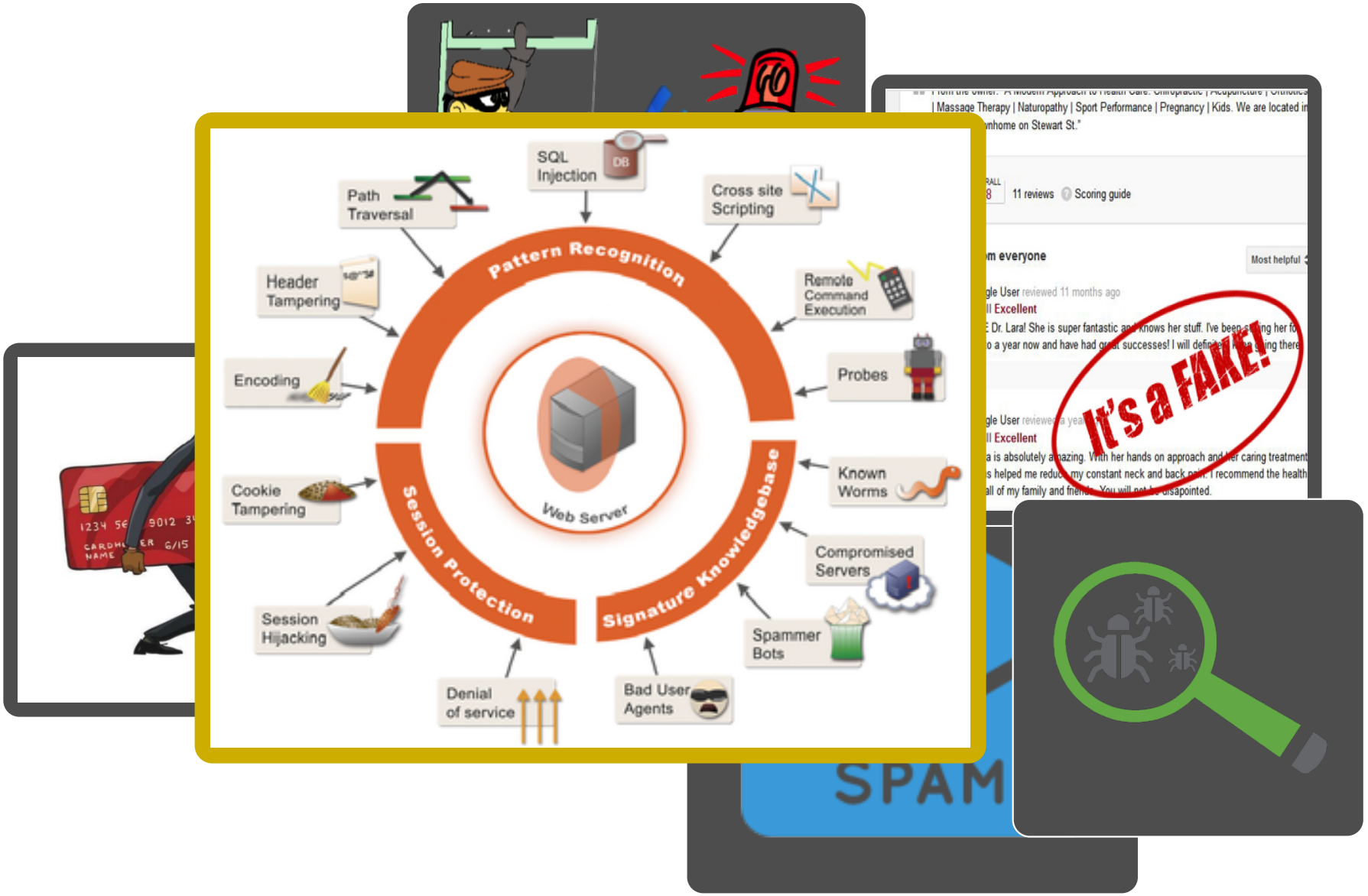

1234 5
9012 3456
CARDH ER 6/15
NAME


SPAM


1234 5
9012 3456
CARDH ER 6/15
NAME

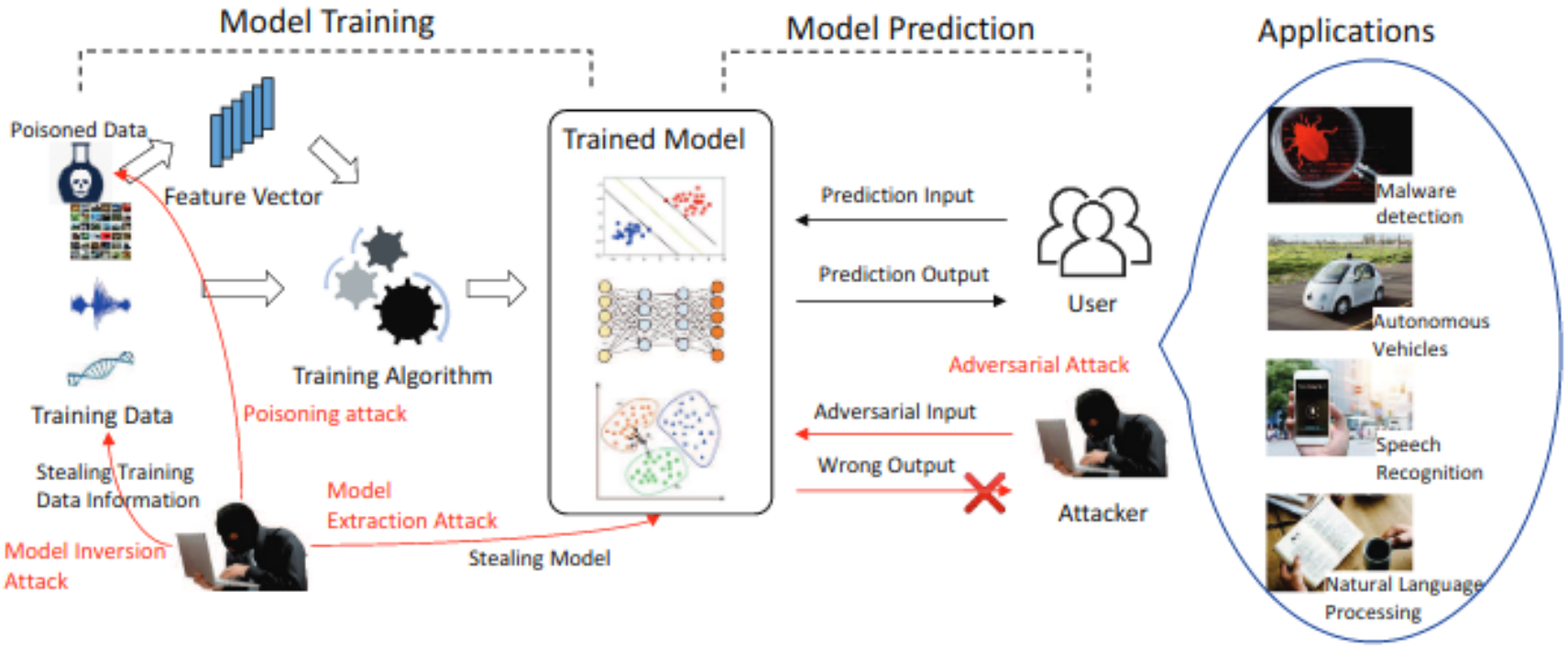

| Massage Therapy | Naturopathy | Sport Performance | Pregnancy | Kids. We are located in
a walk-up townhome on Stewart St."
SCORE
OVERALL
28
11 reviews
Scoring guide
11 Reviews from everyone
Most helpful
A Google User reviewed 11 months ago
Overall Excellent
I LOVE Dr. Lara! She is super fantastic and knows her stuff. I've been seeing her for
close to a year now and have had great successes! I will definitely keep seeing there
A Google User
Overall Excellent
Dr. Lara is absolutely amazing. With her hands on approach and her caring treatment
she has helped me reduce my constant neck and back pain. I recommend the health
loft to all of my family and friends. You will not be disapointed.
It's a FAKE!


SPAM


SQL Injection
Path Traversal
Cross site Scripting
Header Tampering
Remote Command Execution
Encoding
Probes
Cookie Tampering
Known Worms
Compromised Servers
Session Hijacking
Spammer Bots
Denial of service
Bad User Agents
Pattern Recognition
Signature Knowledgebase
Session Protection
Web Server
It's a FAKE!
SPAM

Gonzalo de la Torre-Abaitua y col. (2021). “A Compression-Based Method for Detecting Anomalies in Textual Data”. En: *Entropy* 23.5, pág. 618

Yingzhe He y col. (2019). "Towards privacy and security of deep learning systems: a survey". En: *arXiv e-prints*, arXiv-1911



Adversarially Robust AI Solutions For Cybersecurity Management

GICP

SPOR

Transforming the world through data science and analytics

ICMAT INSTITUTO DE CIENCIAS MATEMÁTICAS

Supporting Cyberinsurance from a Behavioural Choice Perspective (CYBECO)

1. Provide new methods for incorporating the nature of adversarial actions in risk calculations for cybersecurity and cyberinsurance: countering lack of attack data through SEJ, better founded risk management approaches in cybersecurity, beyond risk matrices, and an integrated framework for deciding cybersecurity investments.
2. Implementation of key aspects of the model and incorporates behavioural cyber security findings
3. A more rigorous framework for deciding cybersecurity investments and the identification of cybersecurity nudges

Data acquisition

Monitoring

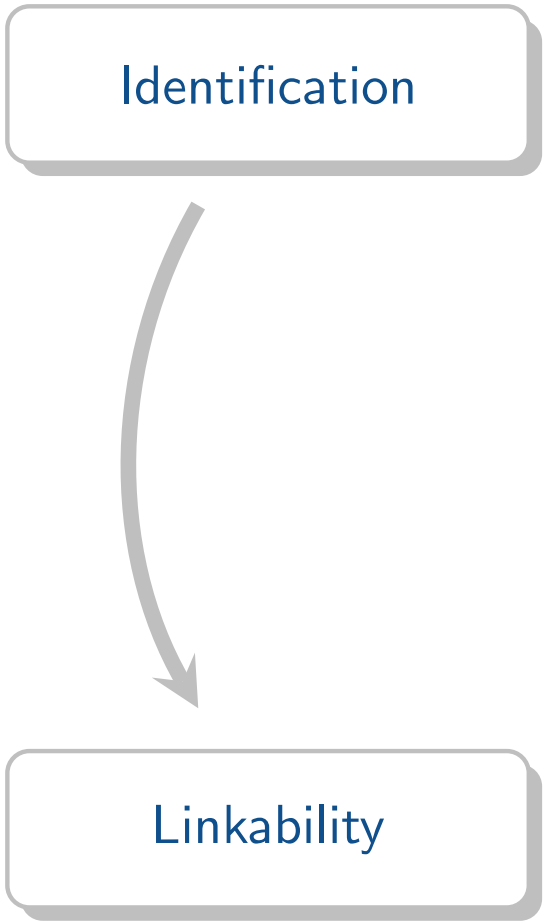
As a byproduct of another activity

Transfer of pre-existing information

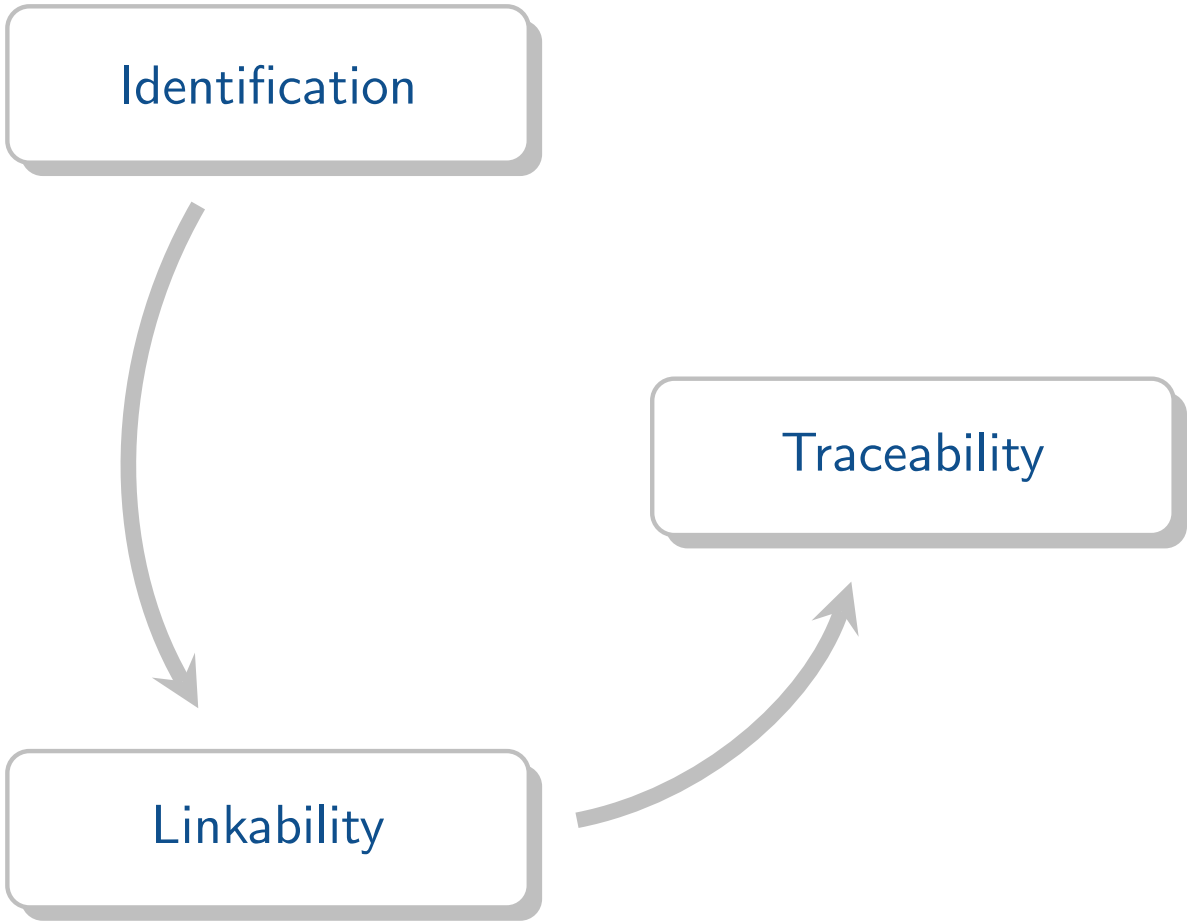
What is that thing called *identity*?

Identification

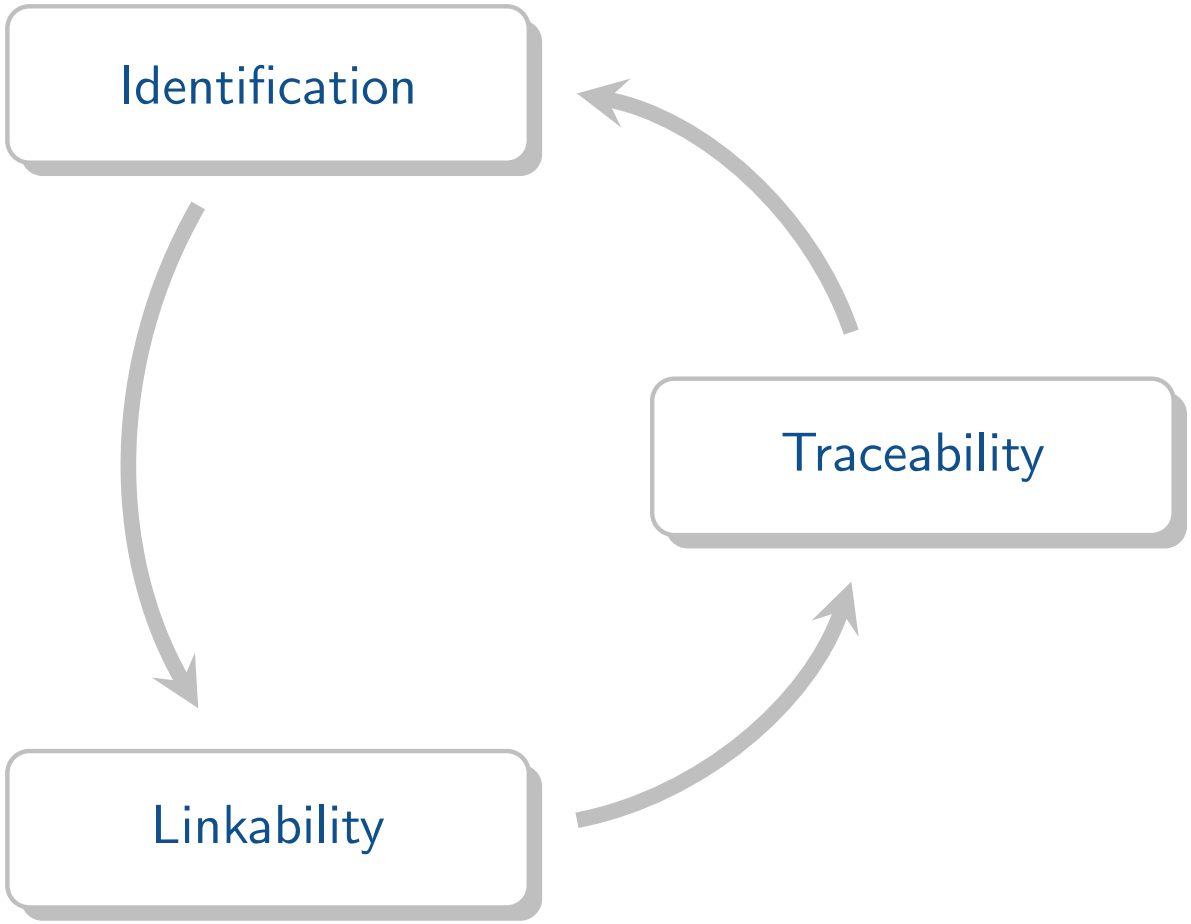
What is that thing called *identity*?



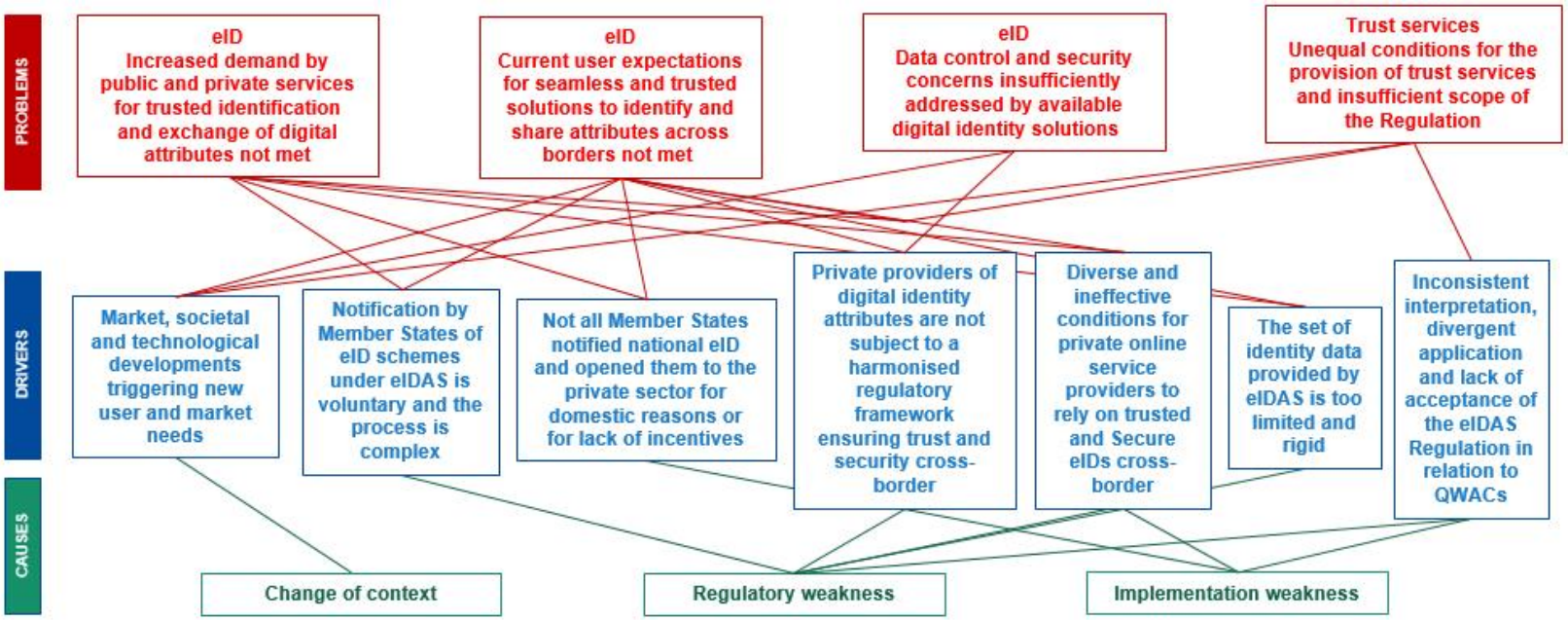
What is that thing called *identity*?



What is that thing called *identity*?



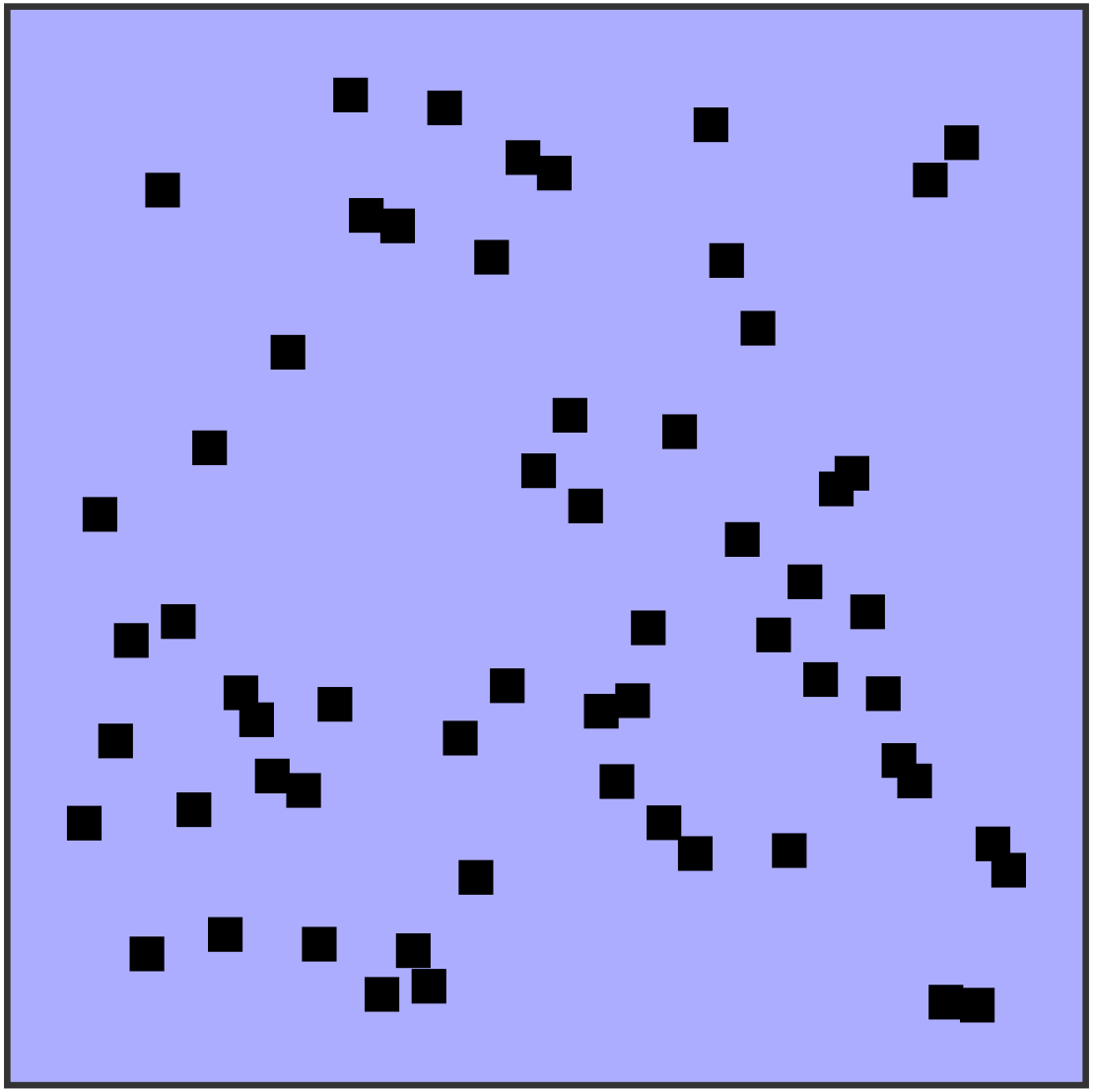
eIDAS (electronic IDentification, Authentication and trust Services)



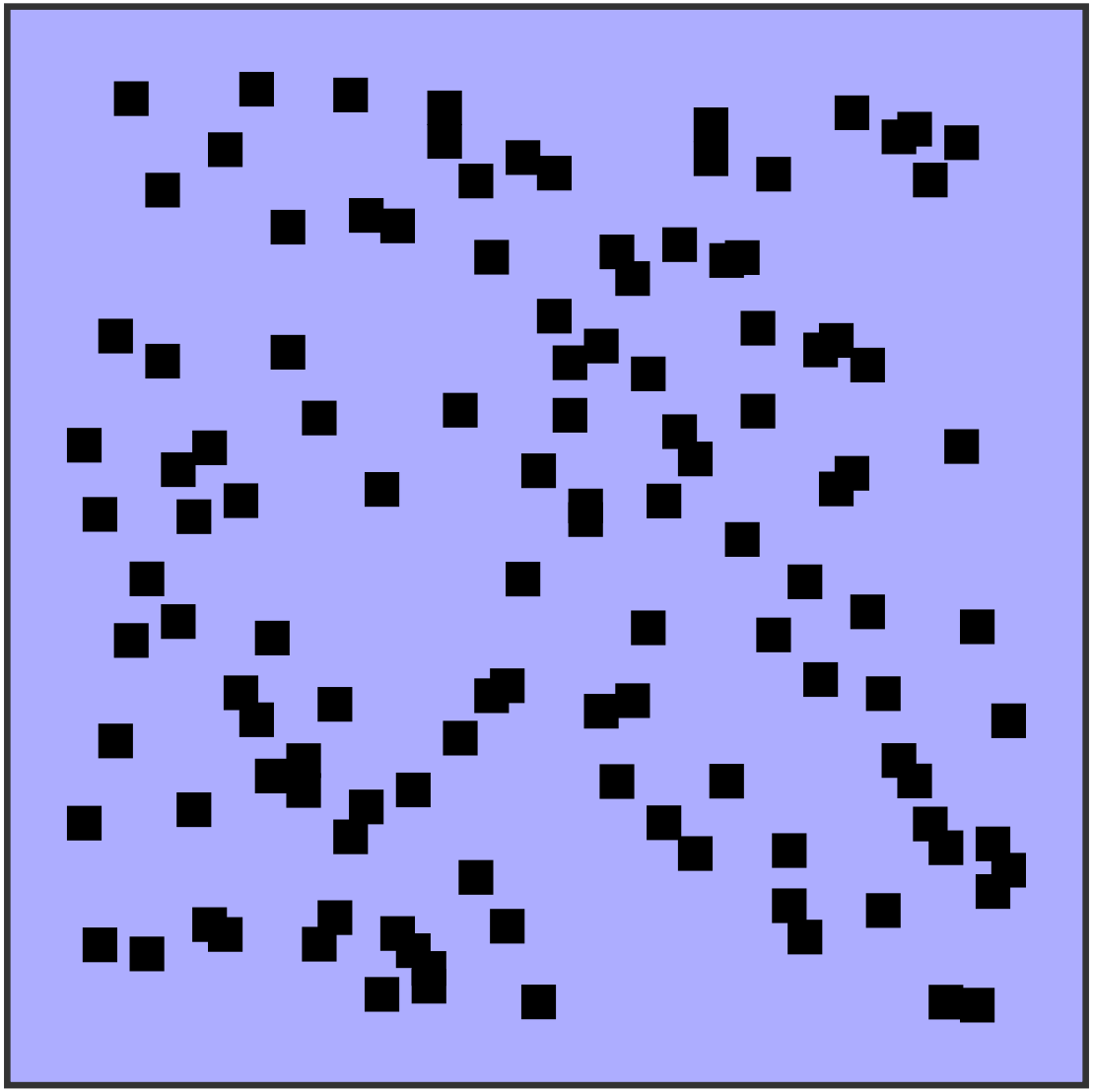
Markets in Crypto-Assets (MiCA) regulation

The Digital Markets Act (DMA)

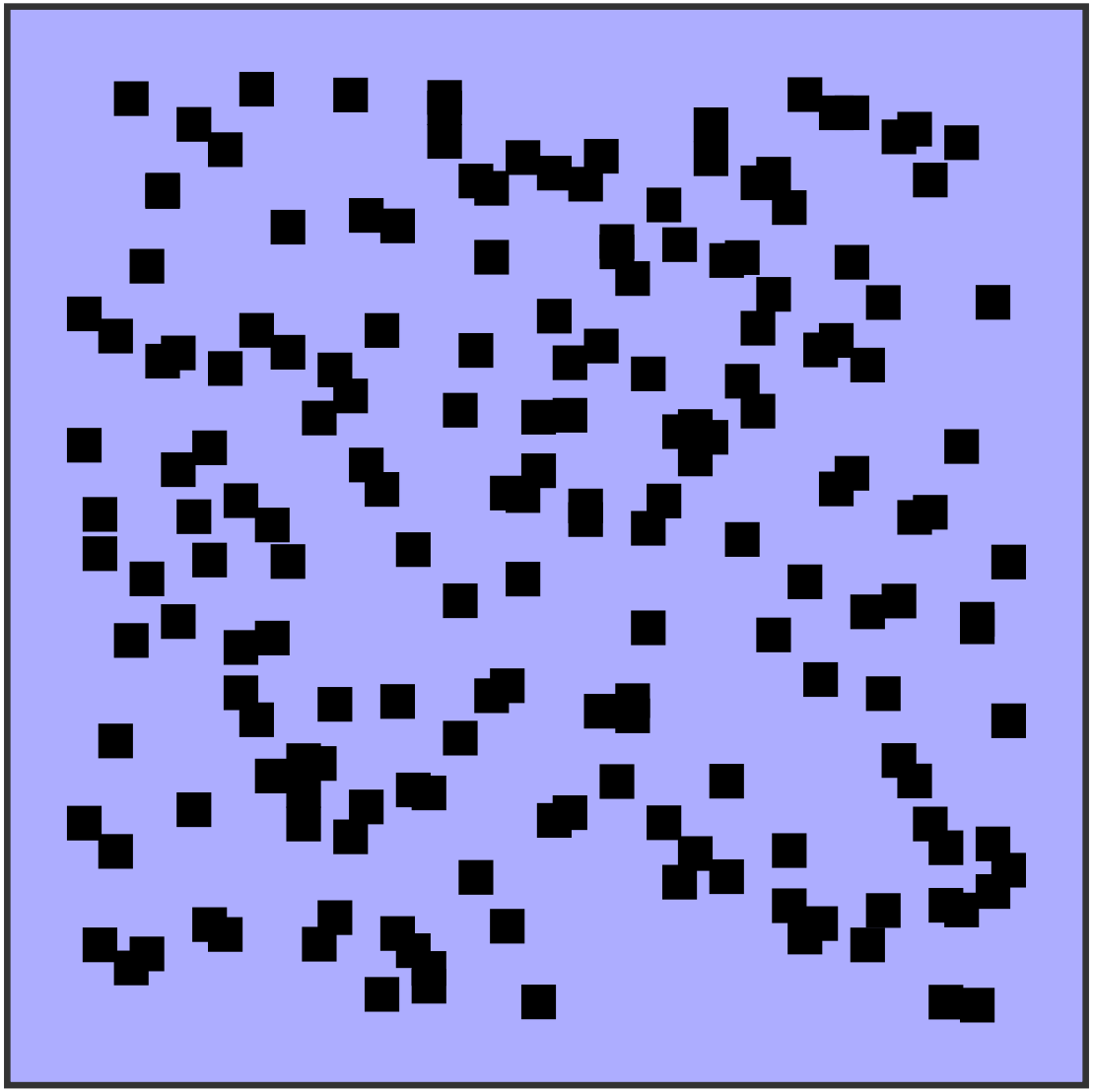
Linkability



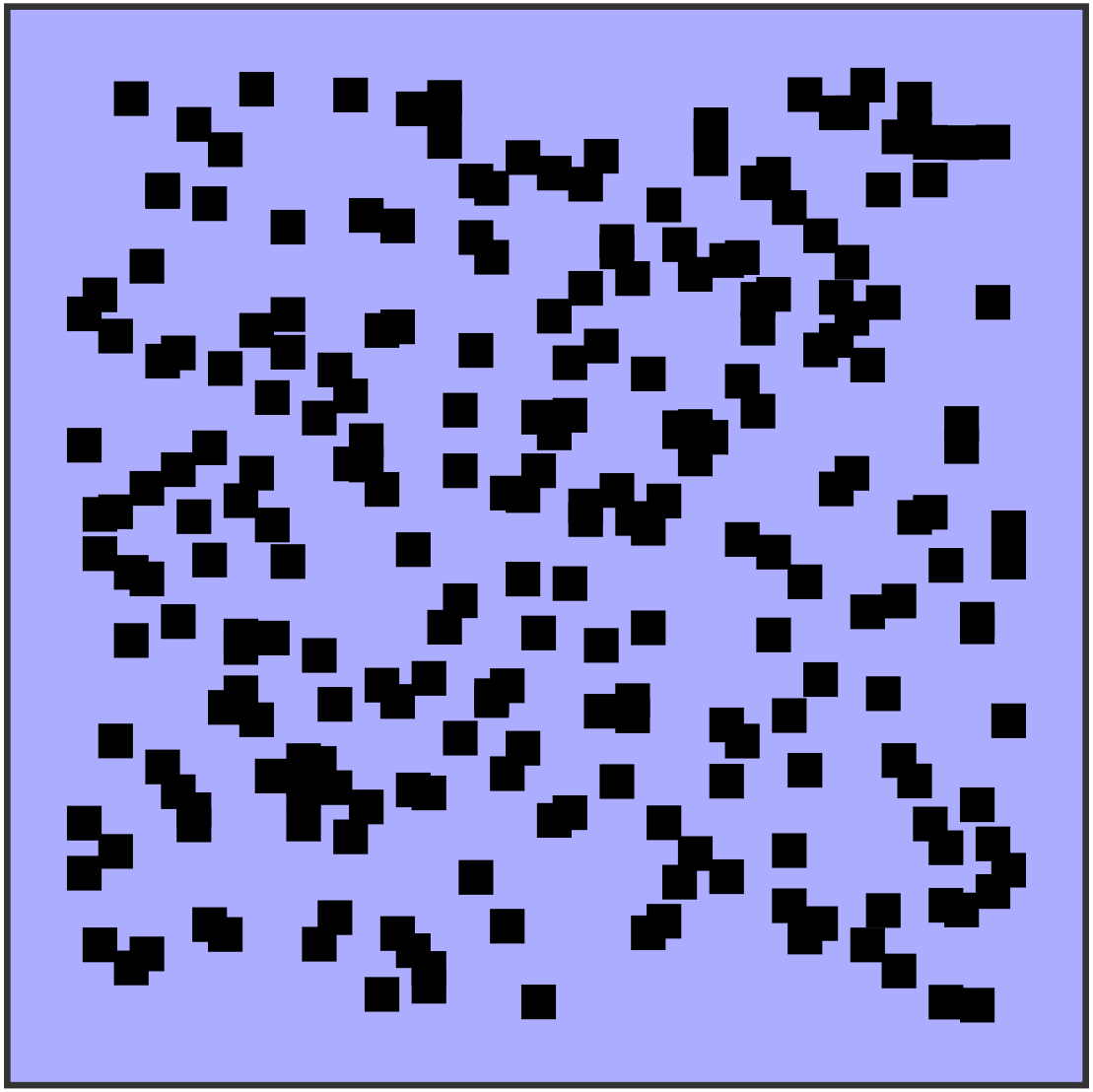
Linkability



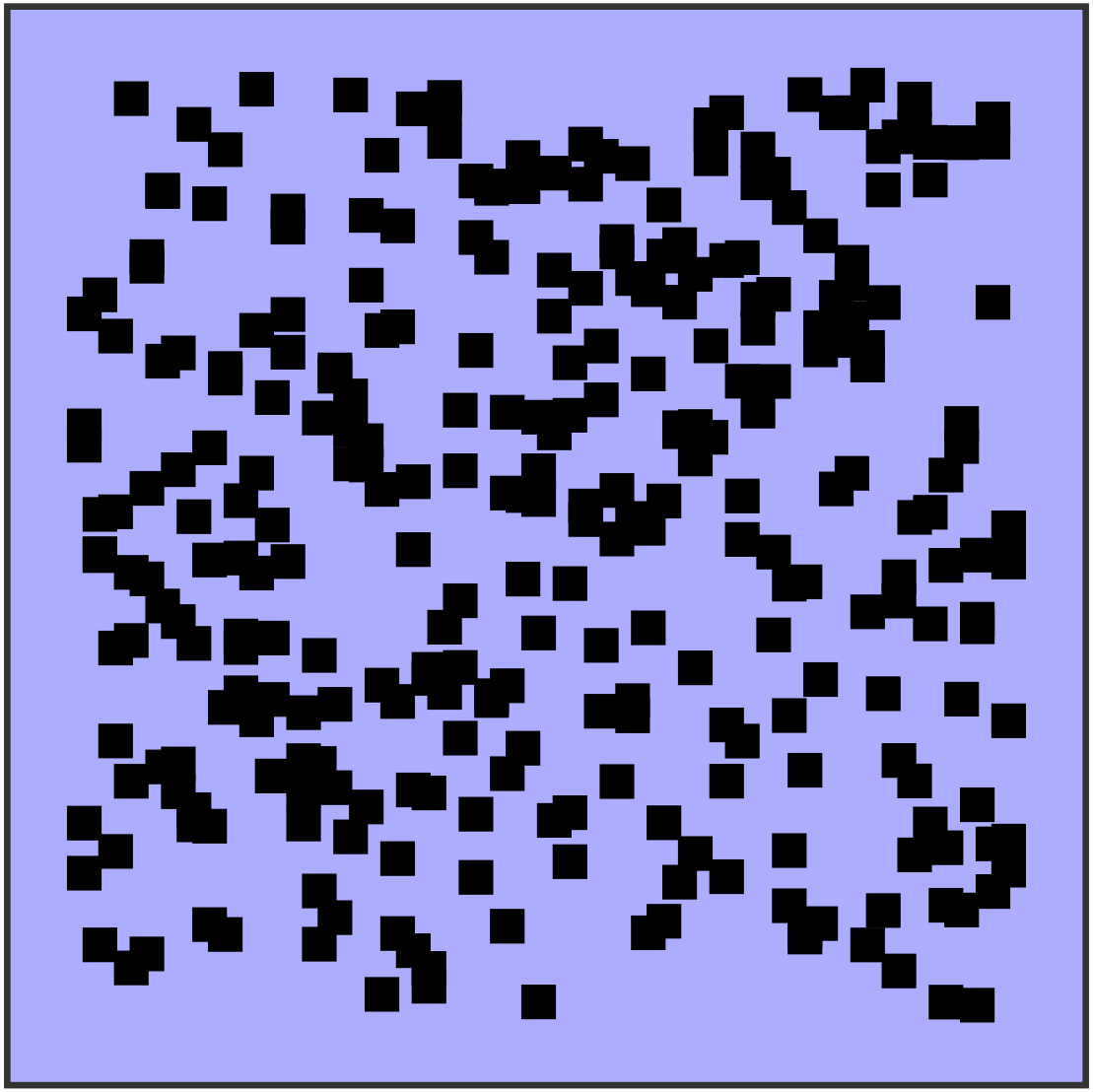
Linkability



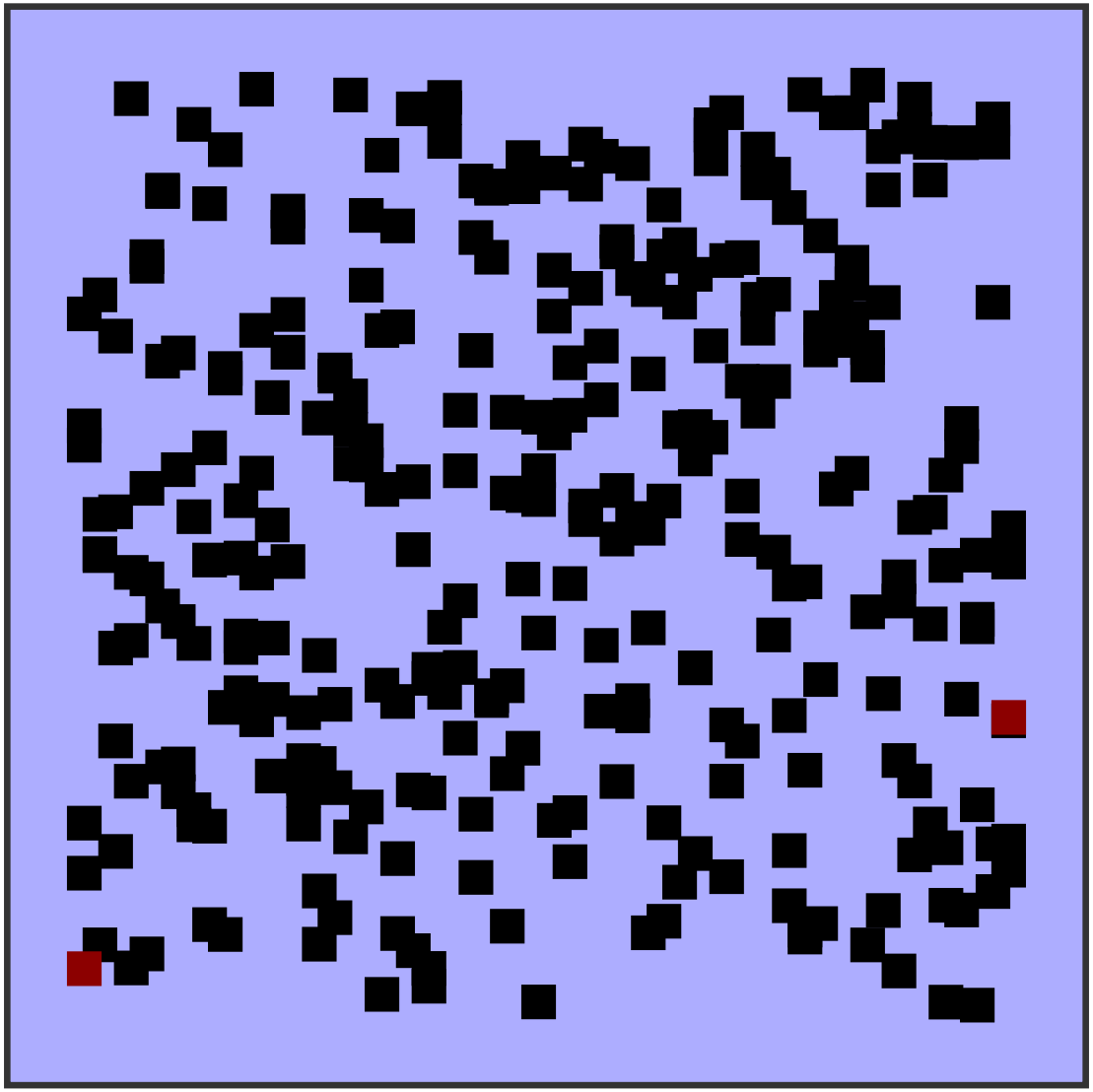
Linkability



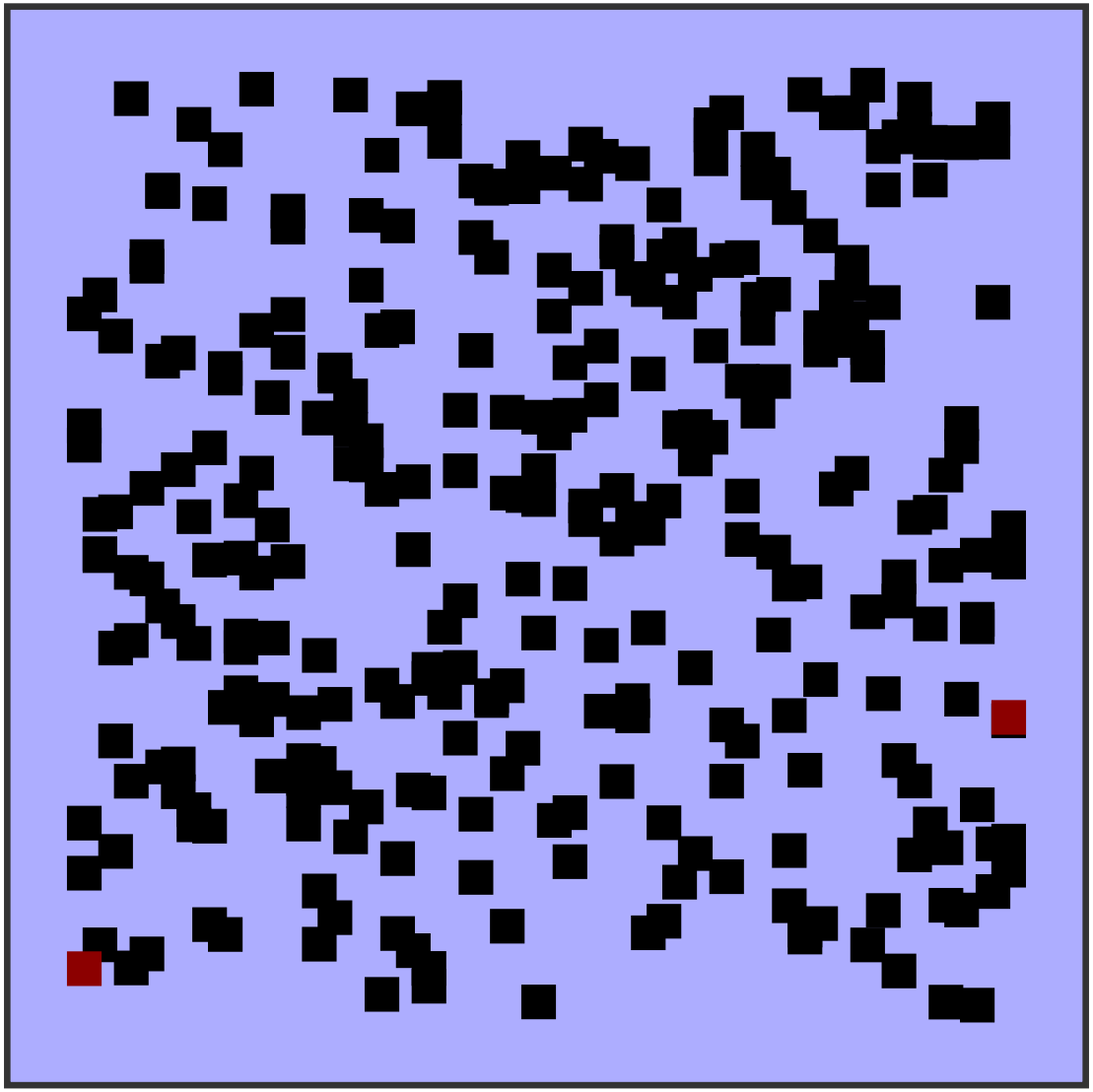
Linkability



Linkability

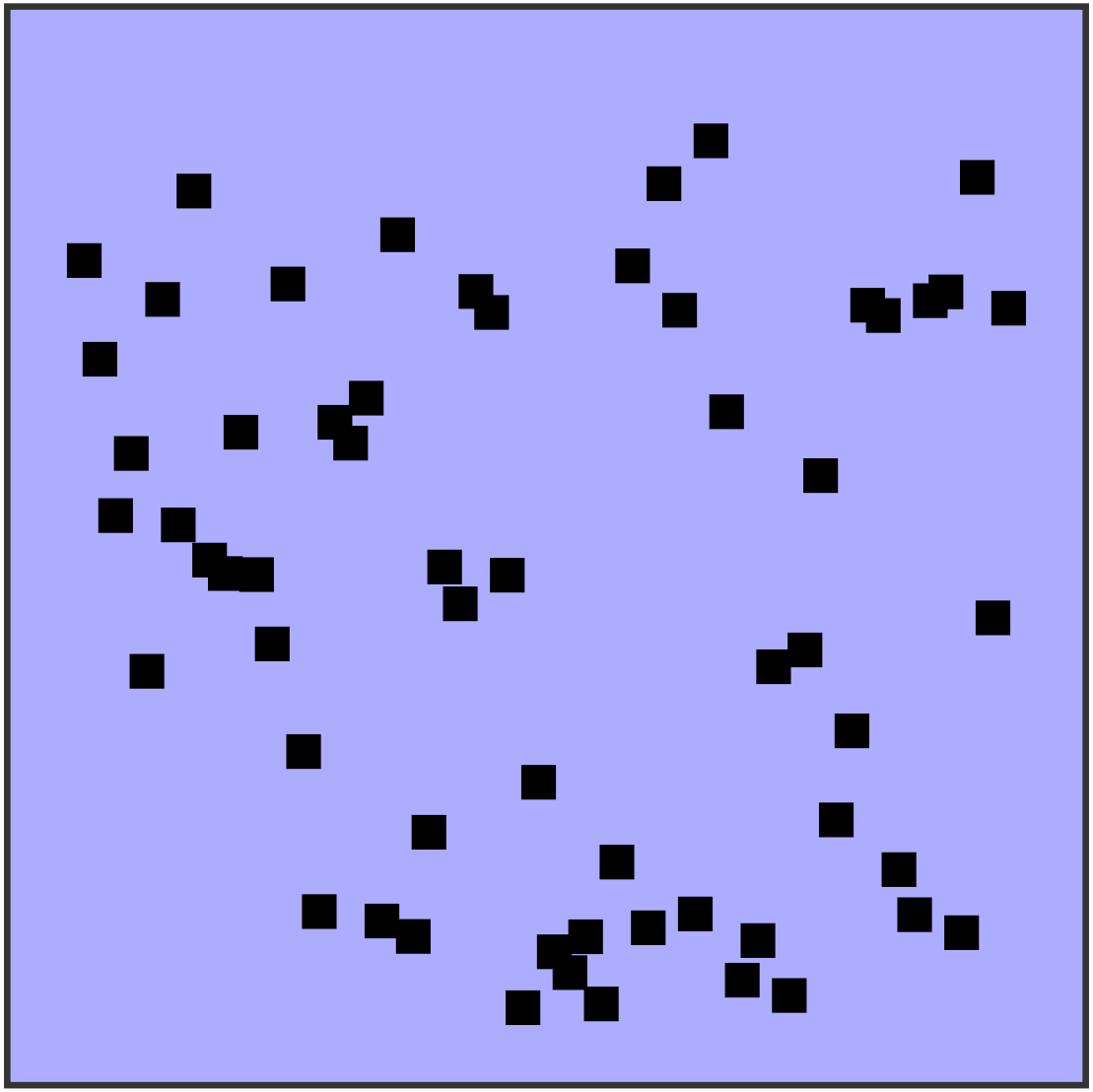


Linkability

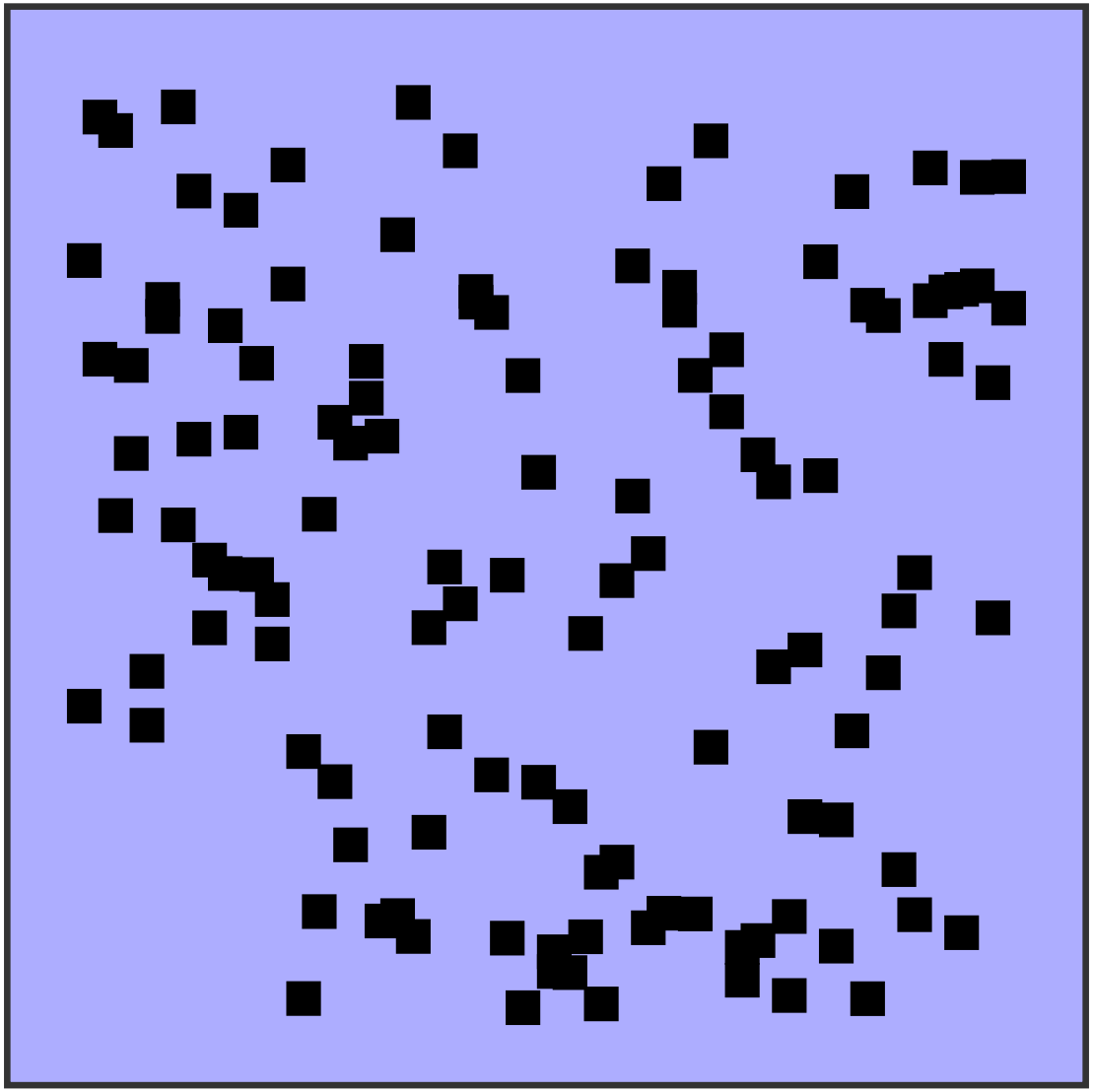


Related???

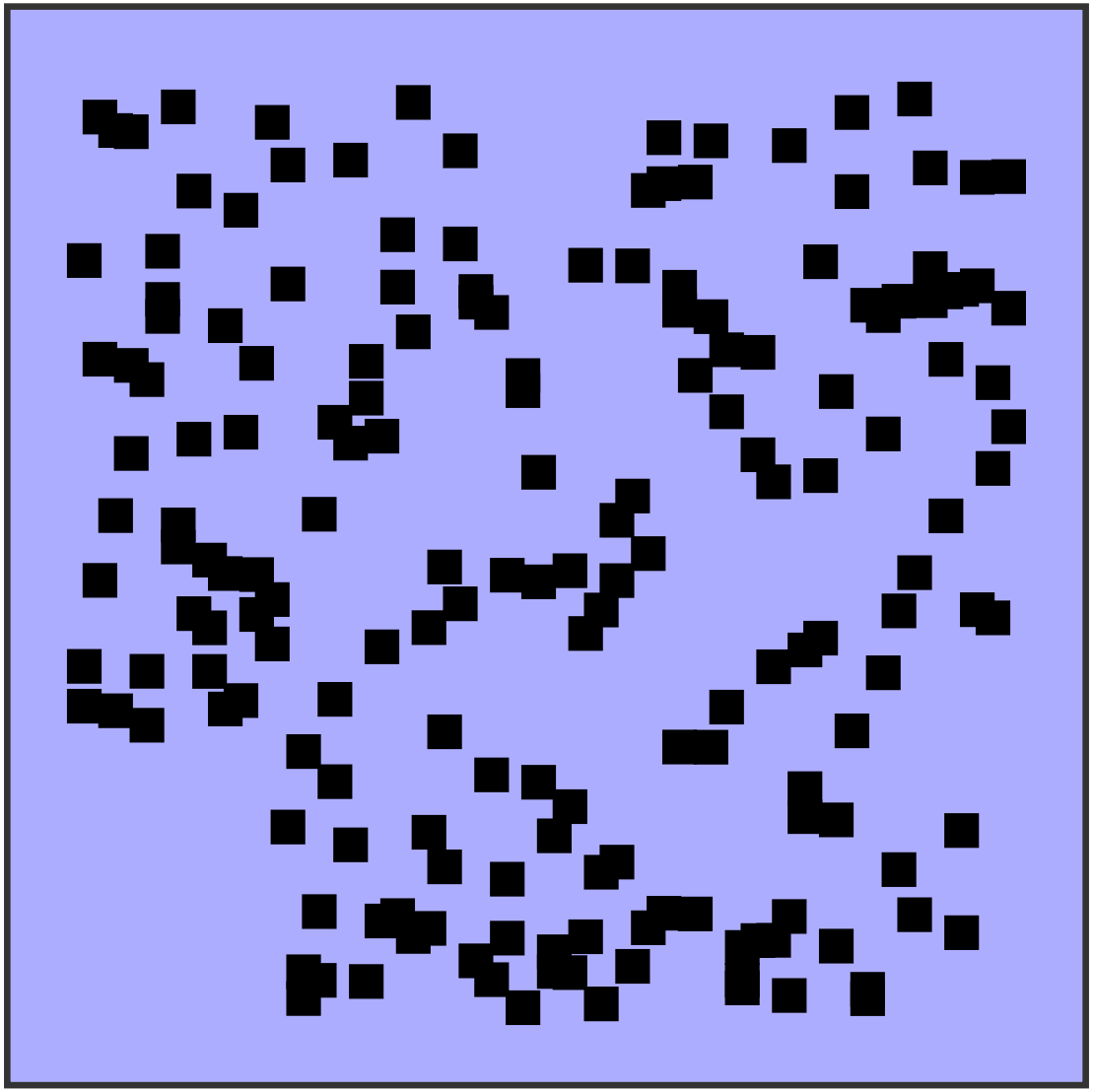
Traceability



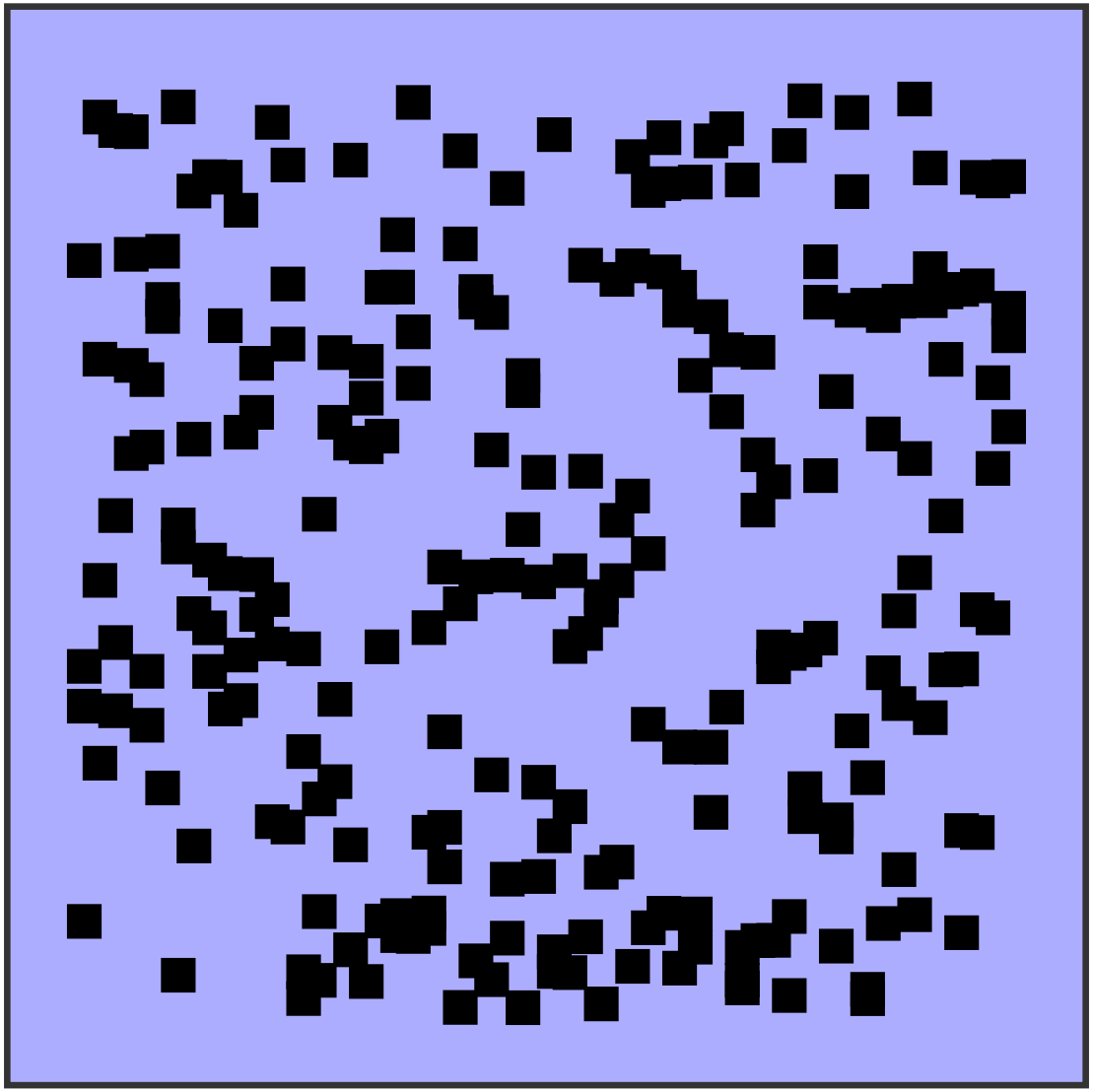
Traceability



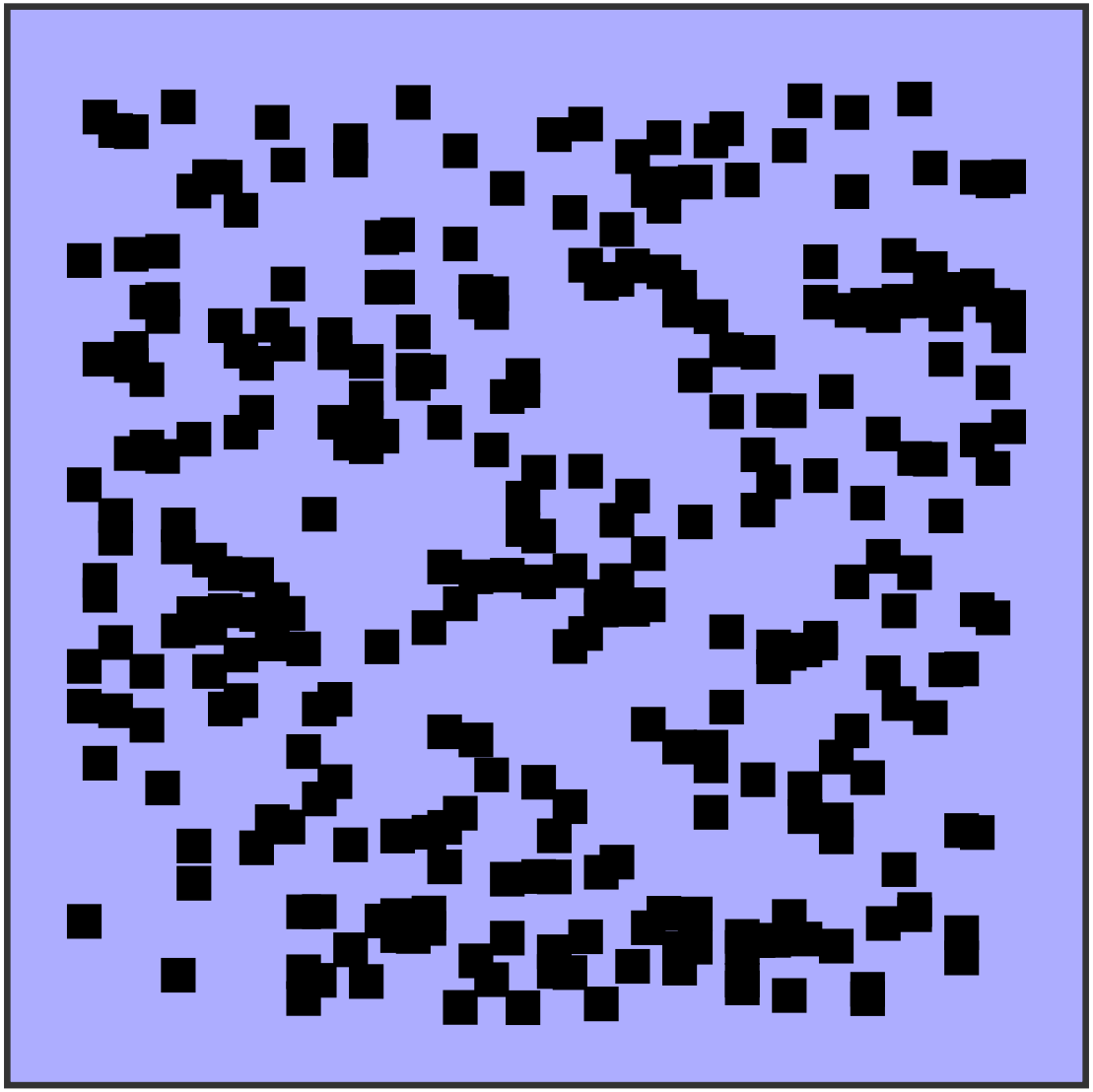
Traceability



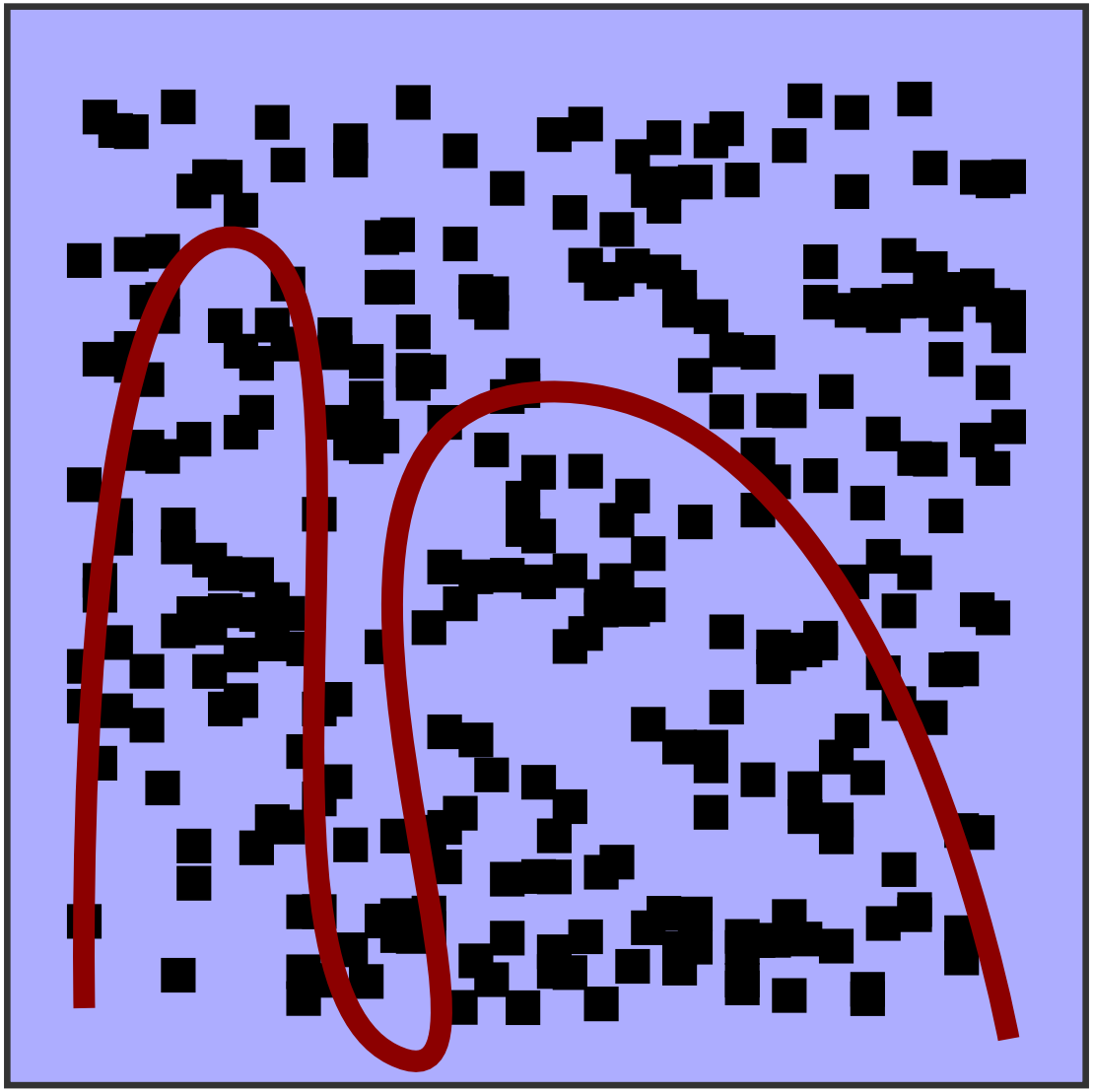
Traceability



Traceability



Traceability



Conventional Digital Signatures

Conventional Digital Signatures	Publicly verifiable, transferable

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anonymous communications

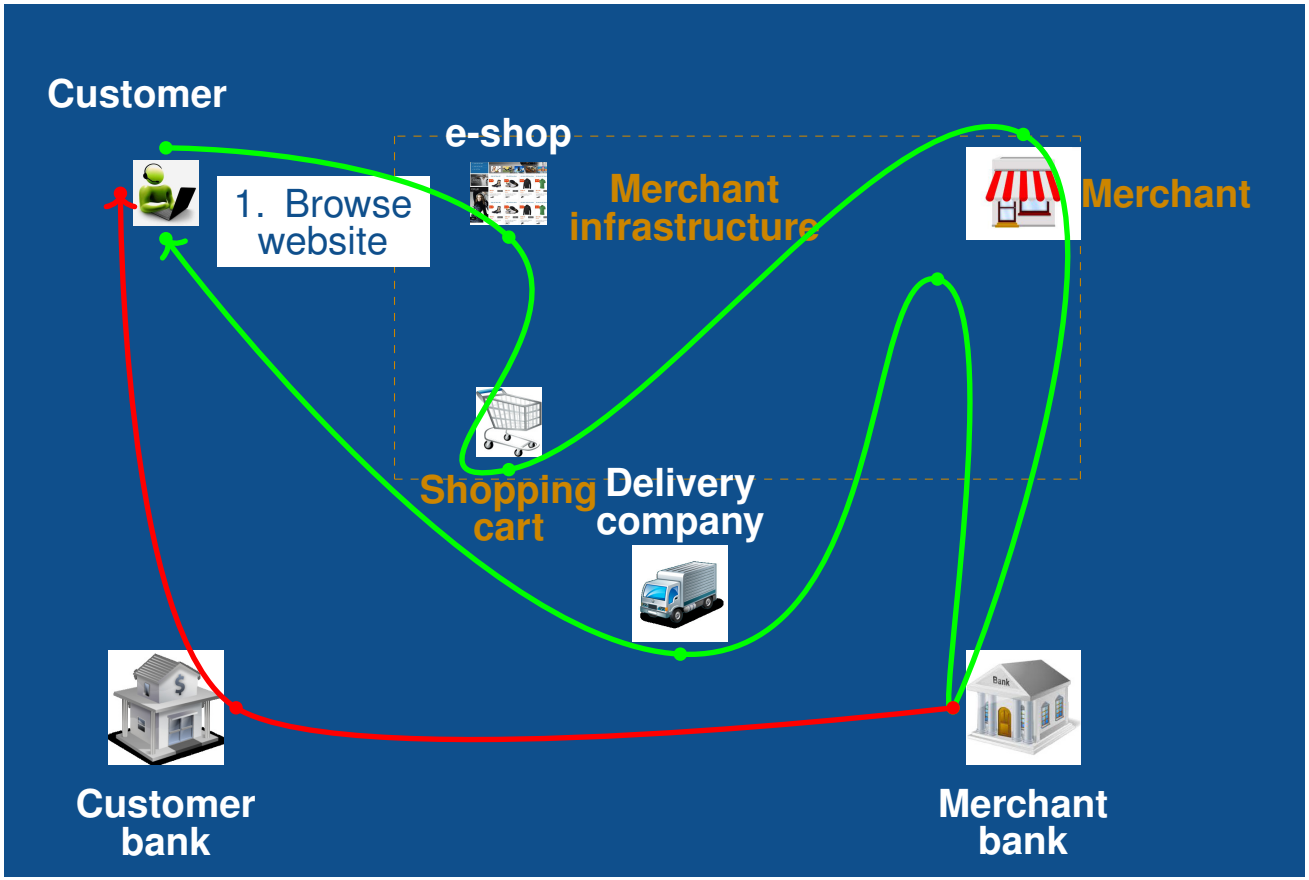
Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anonymous communications
Traceability	

Conventional Digital Signatures	Publicly verifiable, transferable
Deniability	e-voting, e-coin
Linkability	Fairness in anonymous communications
Traceability	promotions in privacy respectul e-commerce

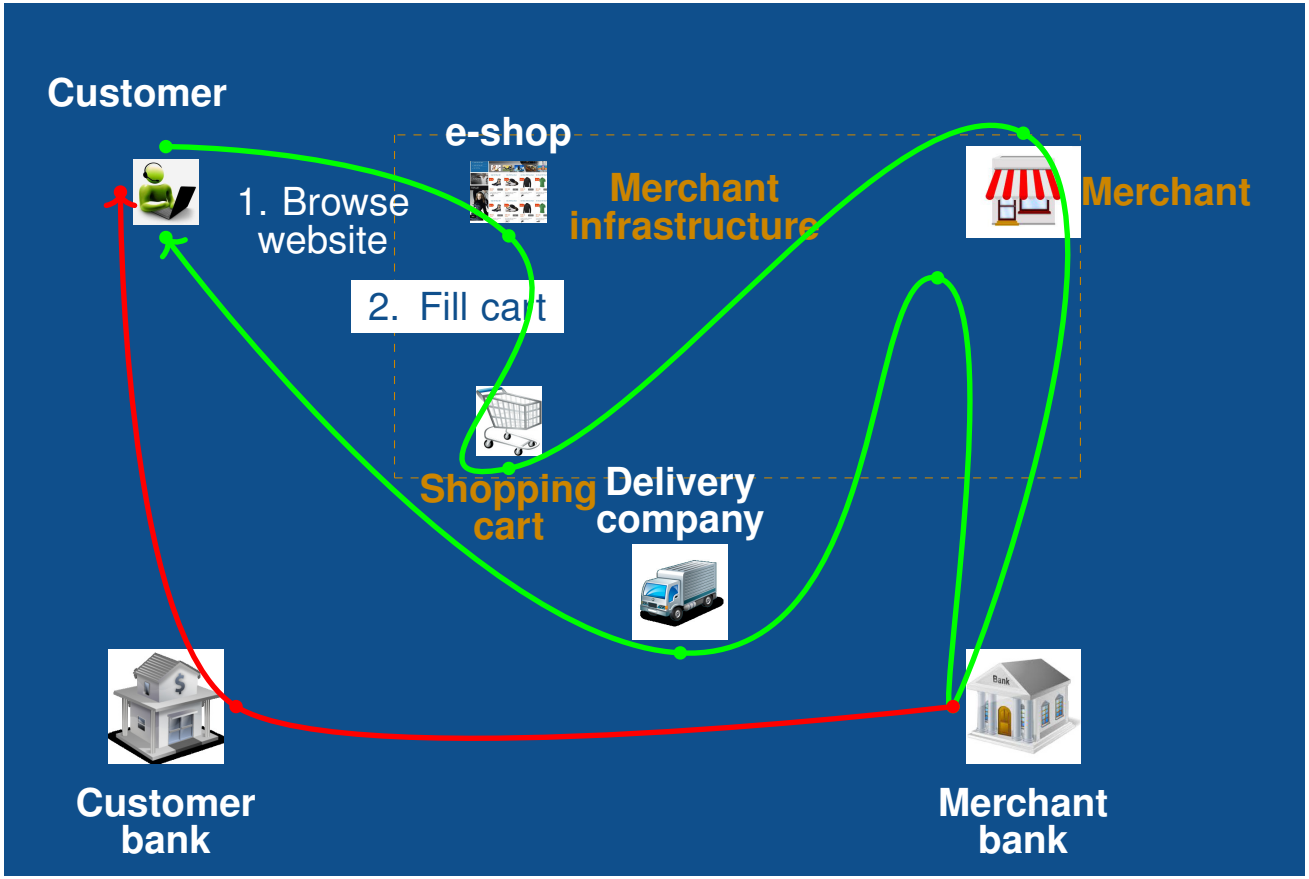
Jesus Diaz, Seung Geol Choi y col. (2019). “A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions”. En: *Advances in Cyber Security: Principles, Techniques, and Applications*. Springer, Singapore, págs. 143-183

Jesus Diaz, David Arroyo y col. (2014). “New x. 509-based mechanisms for fair anonymity management”. En: *Computers & Security* 46, págs. 111-125

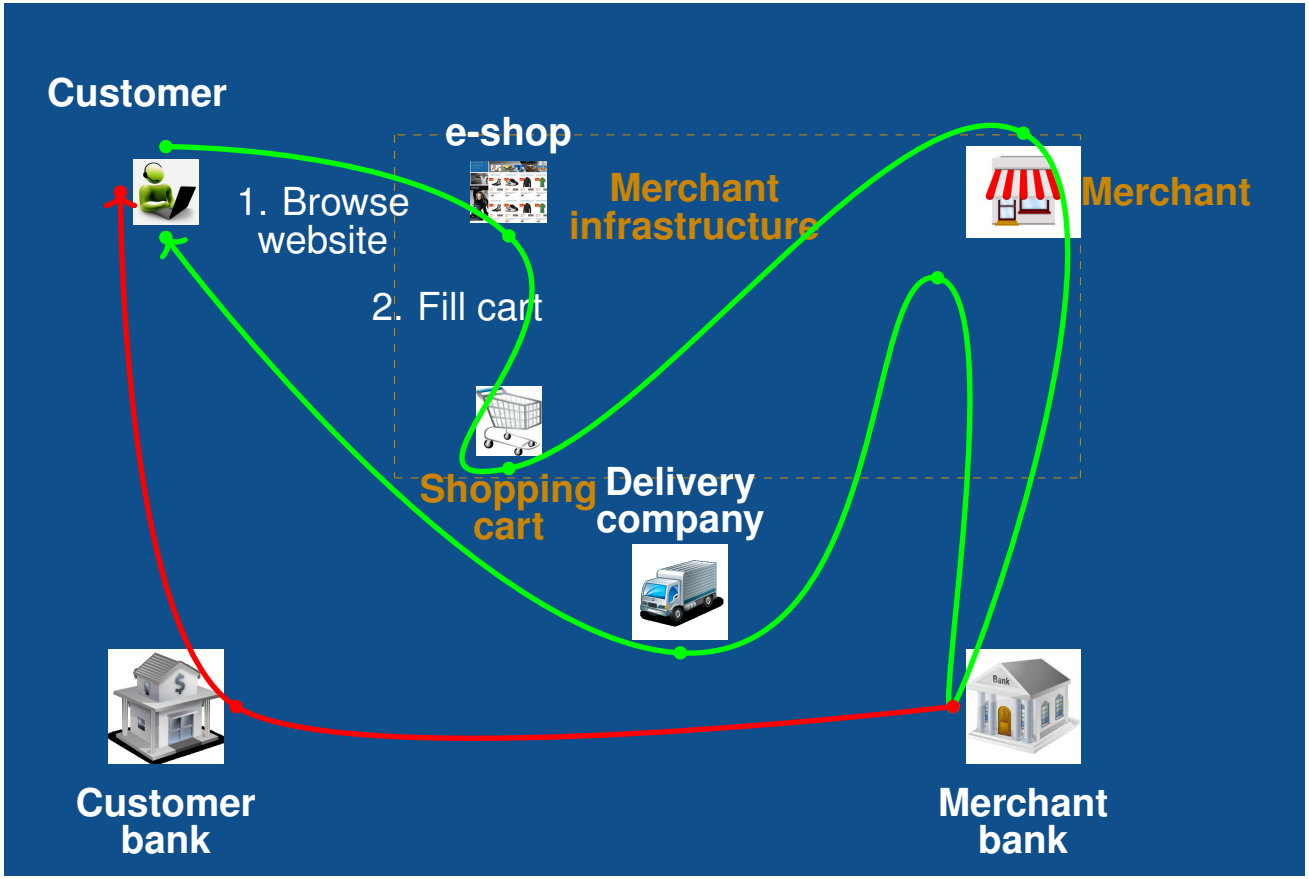
E-shopping process



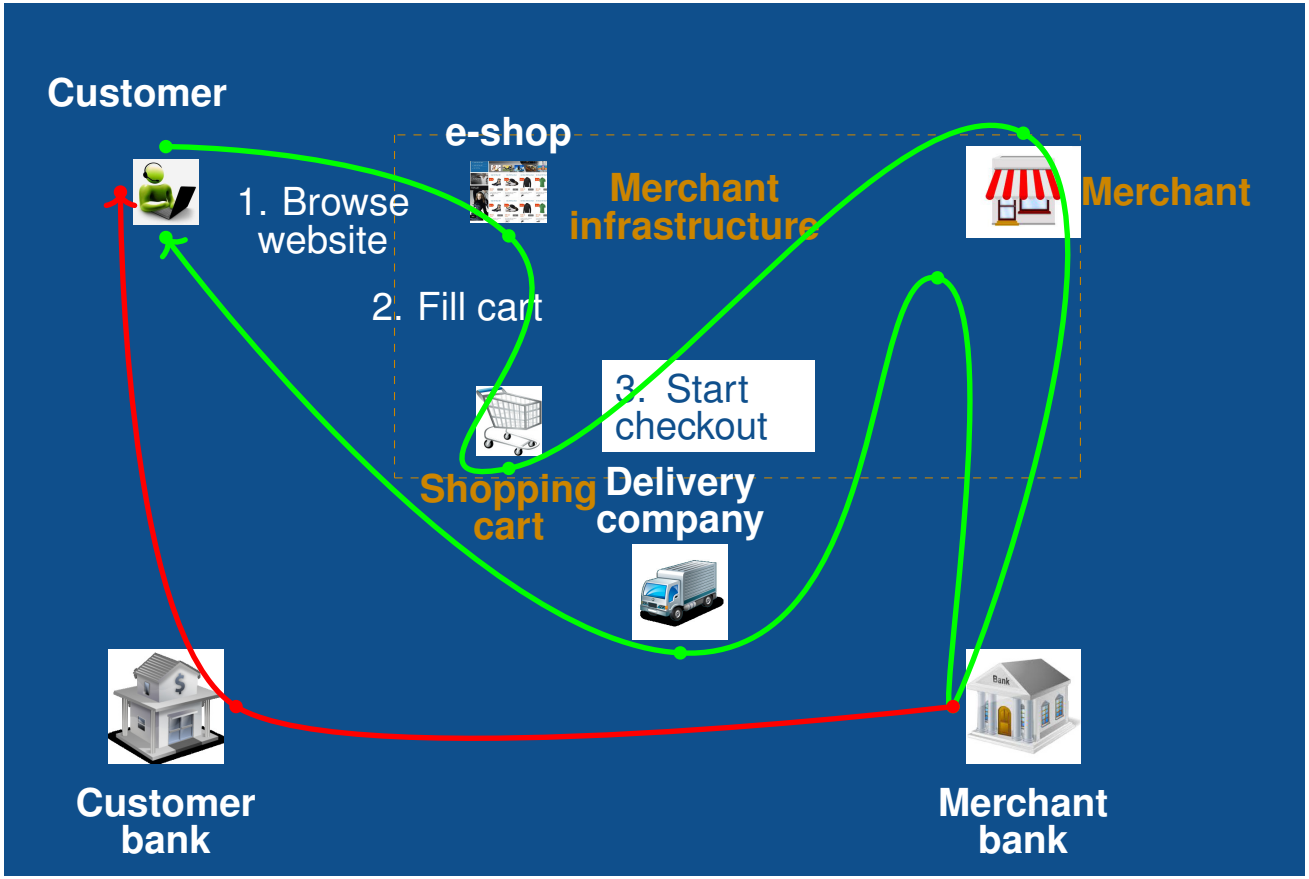
E-shopping process



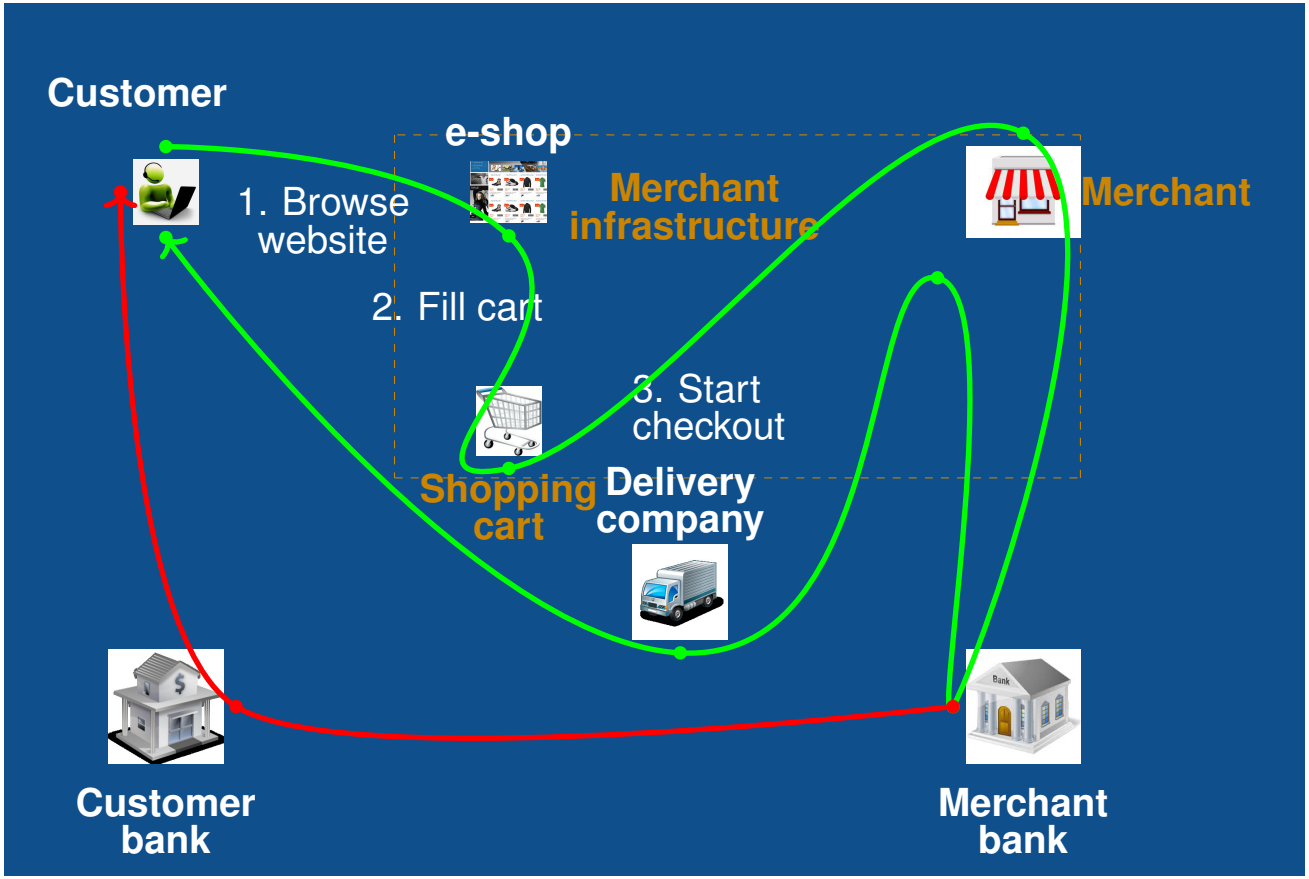
E-shopping process



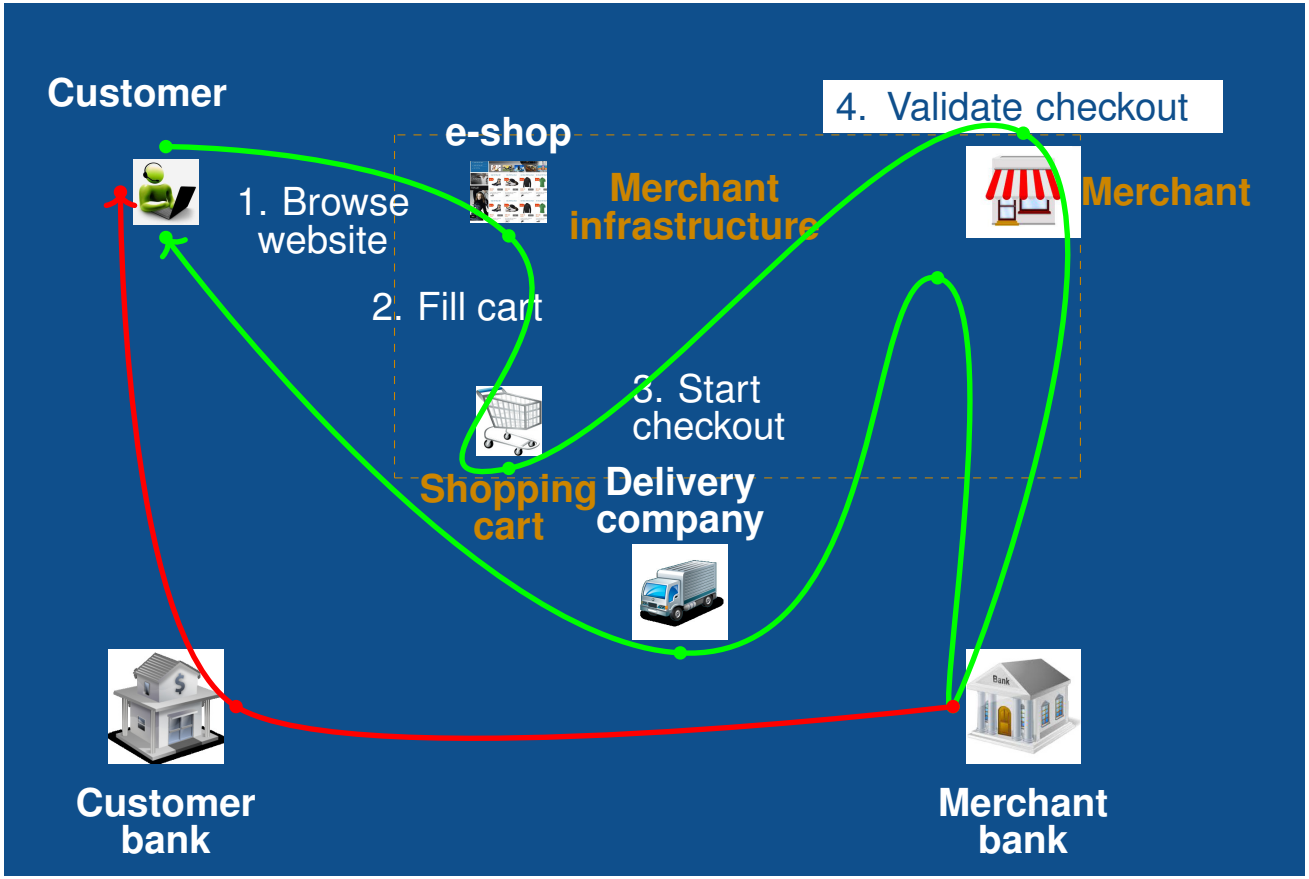
E-shopping process



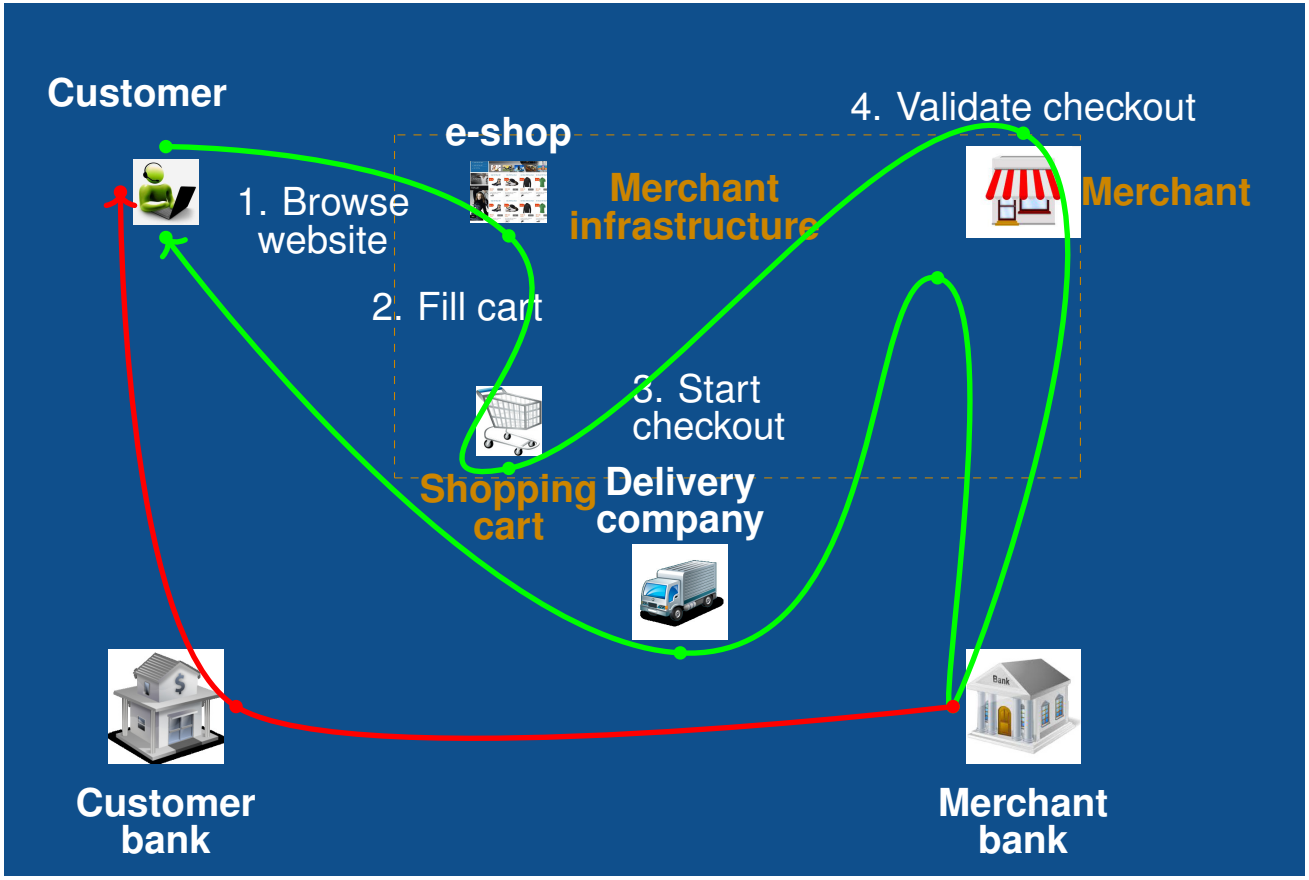
E-shopping process



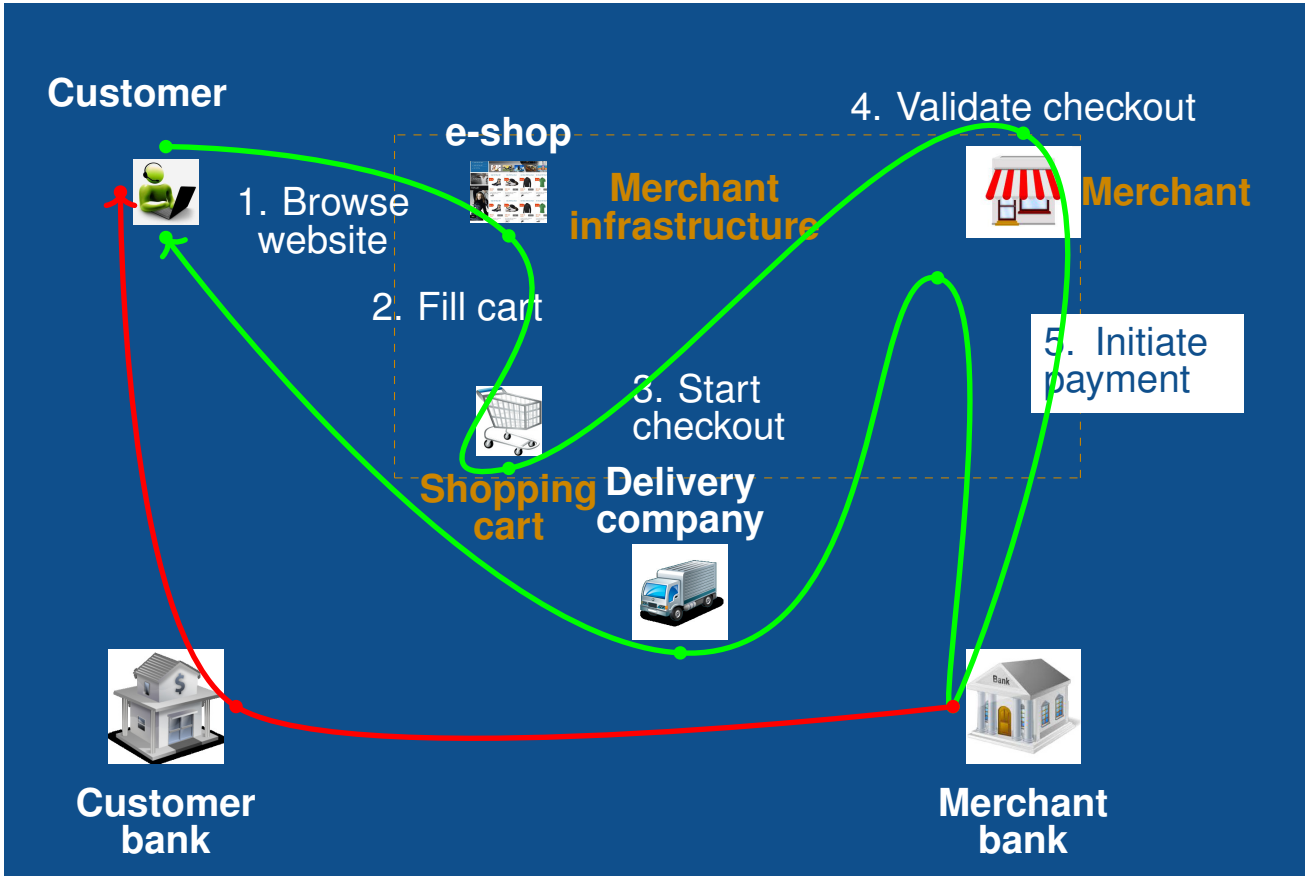
E-shopping process



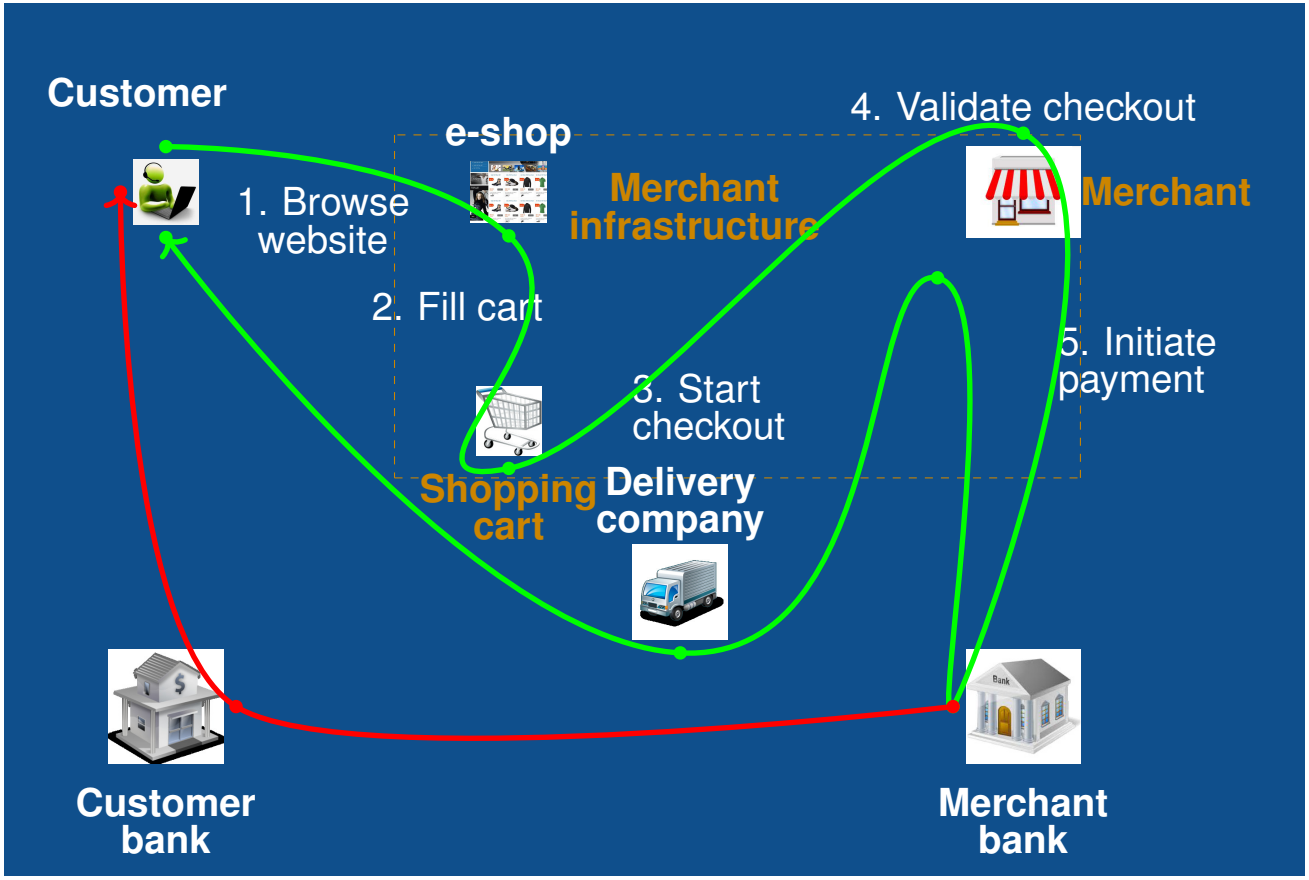
E-shopping process



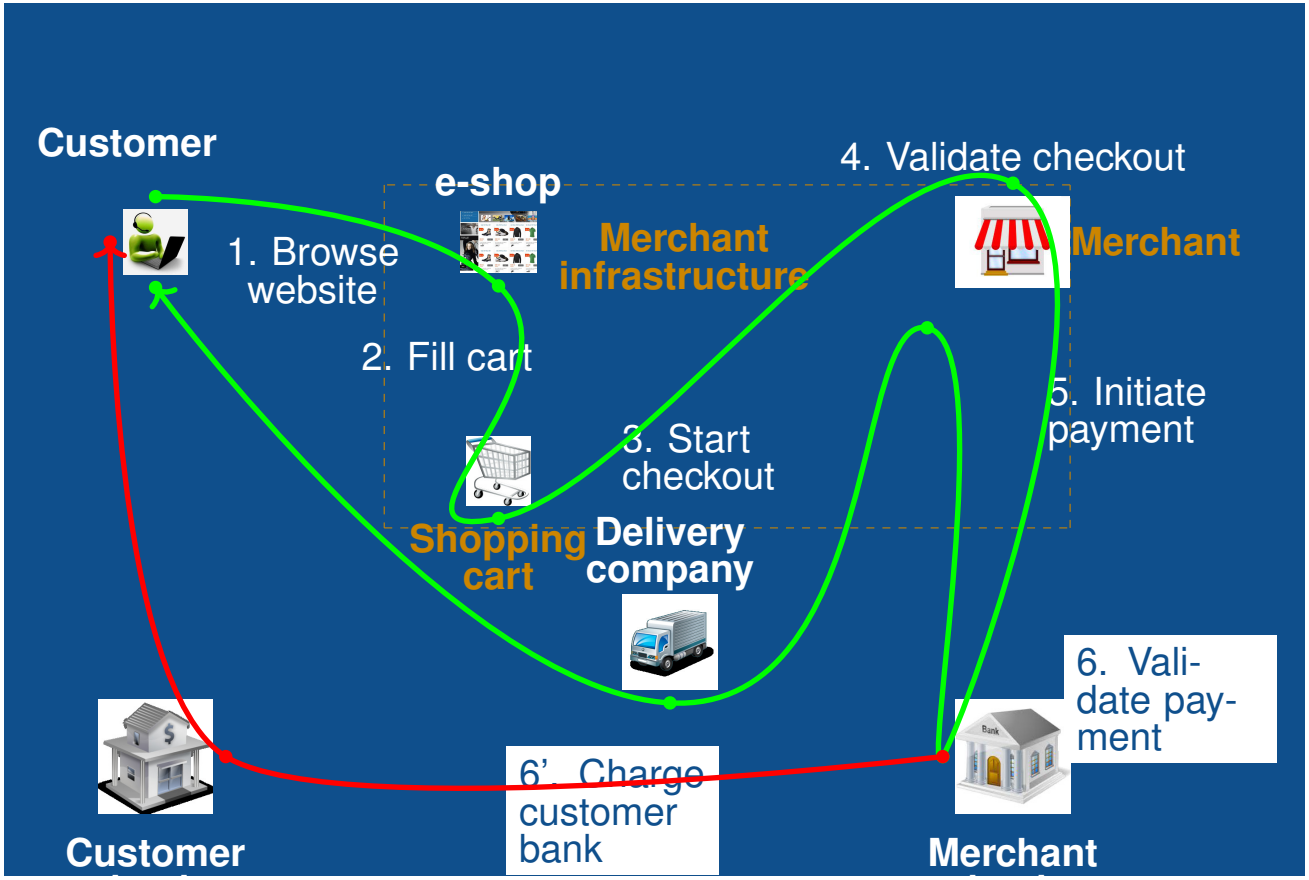
E-shopping process



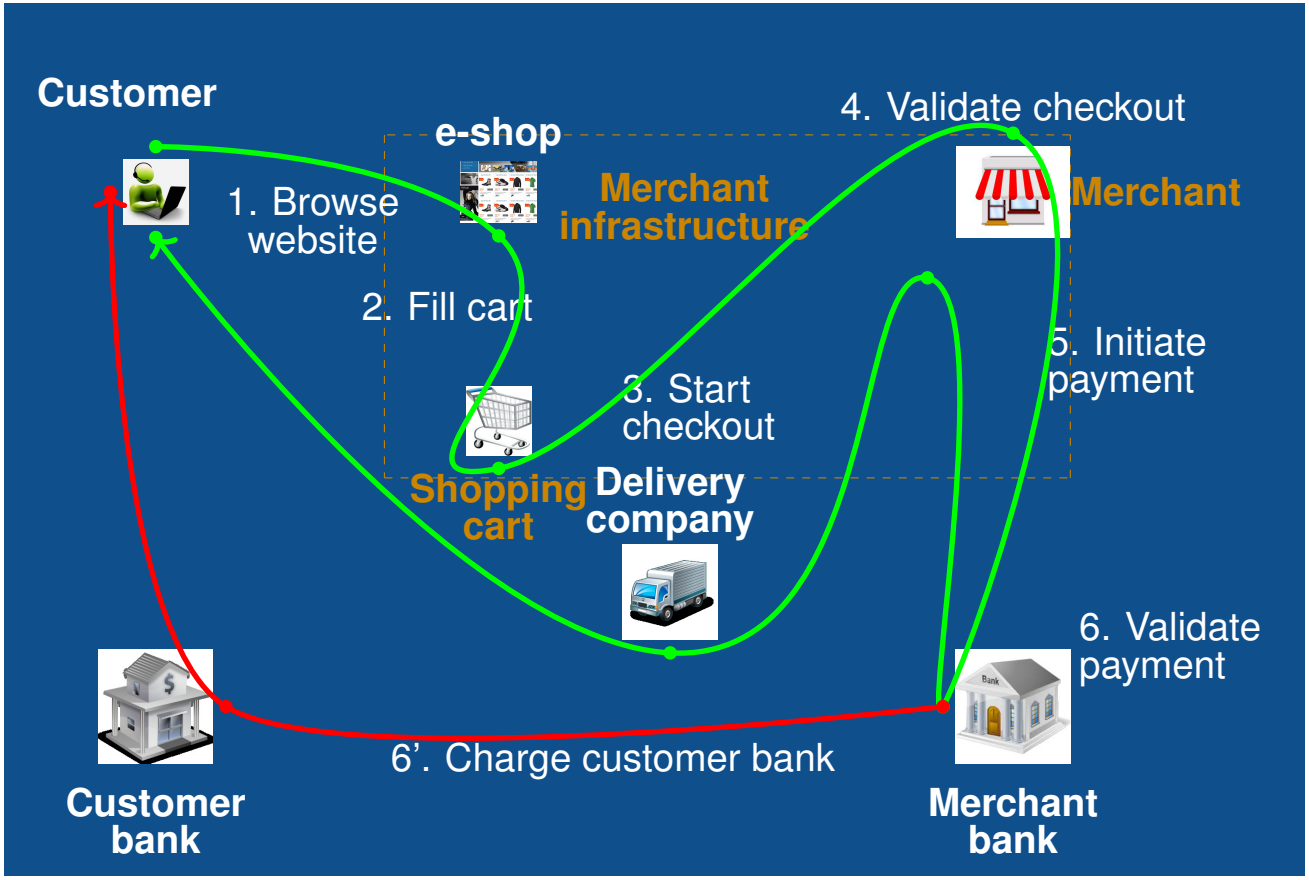
E-shopping process



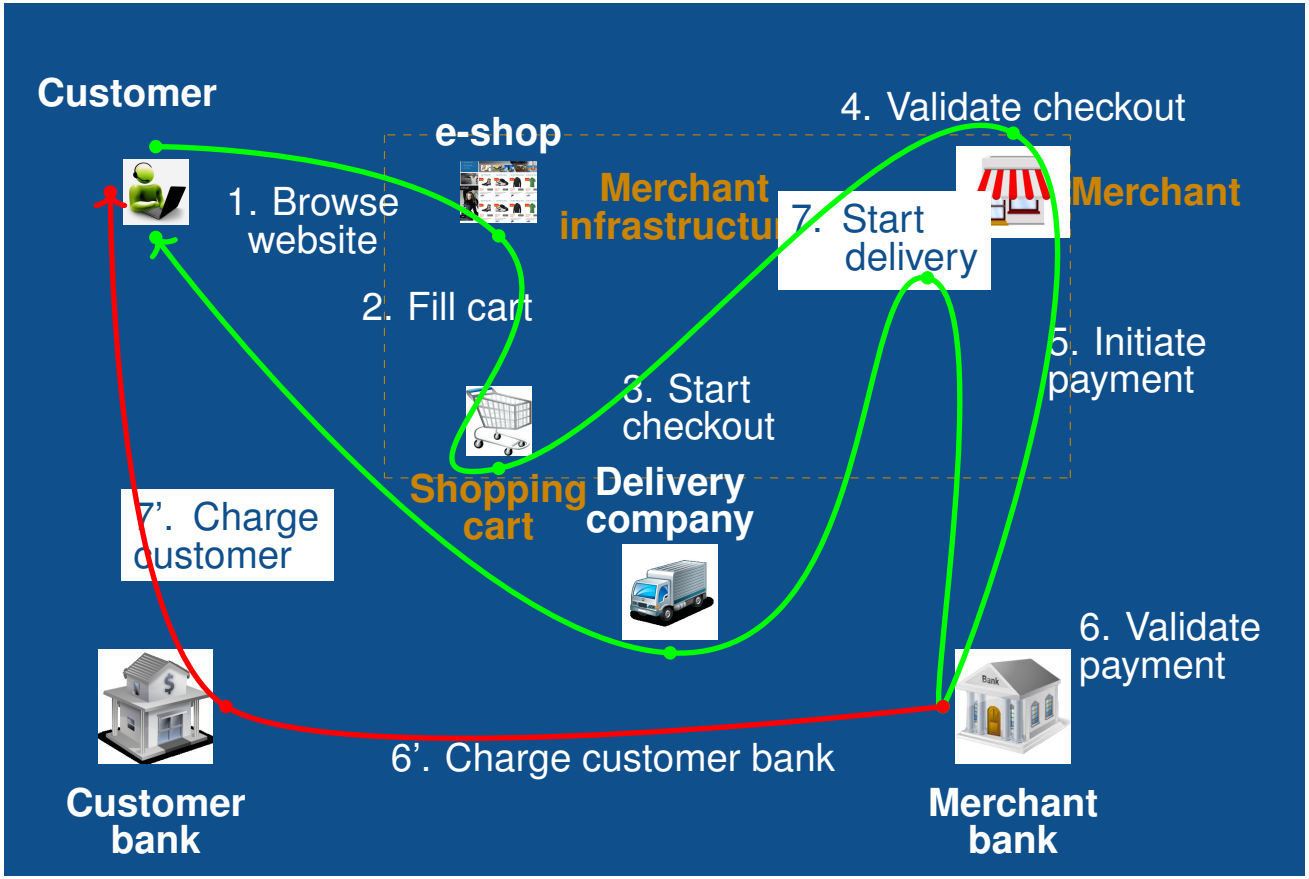
E-shopping process



E-shopping process



E-shopping process



Methodology

PRIVACY

+ Compatibility
+ Utility

Methodology

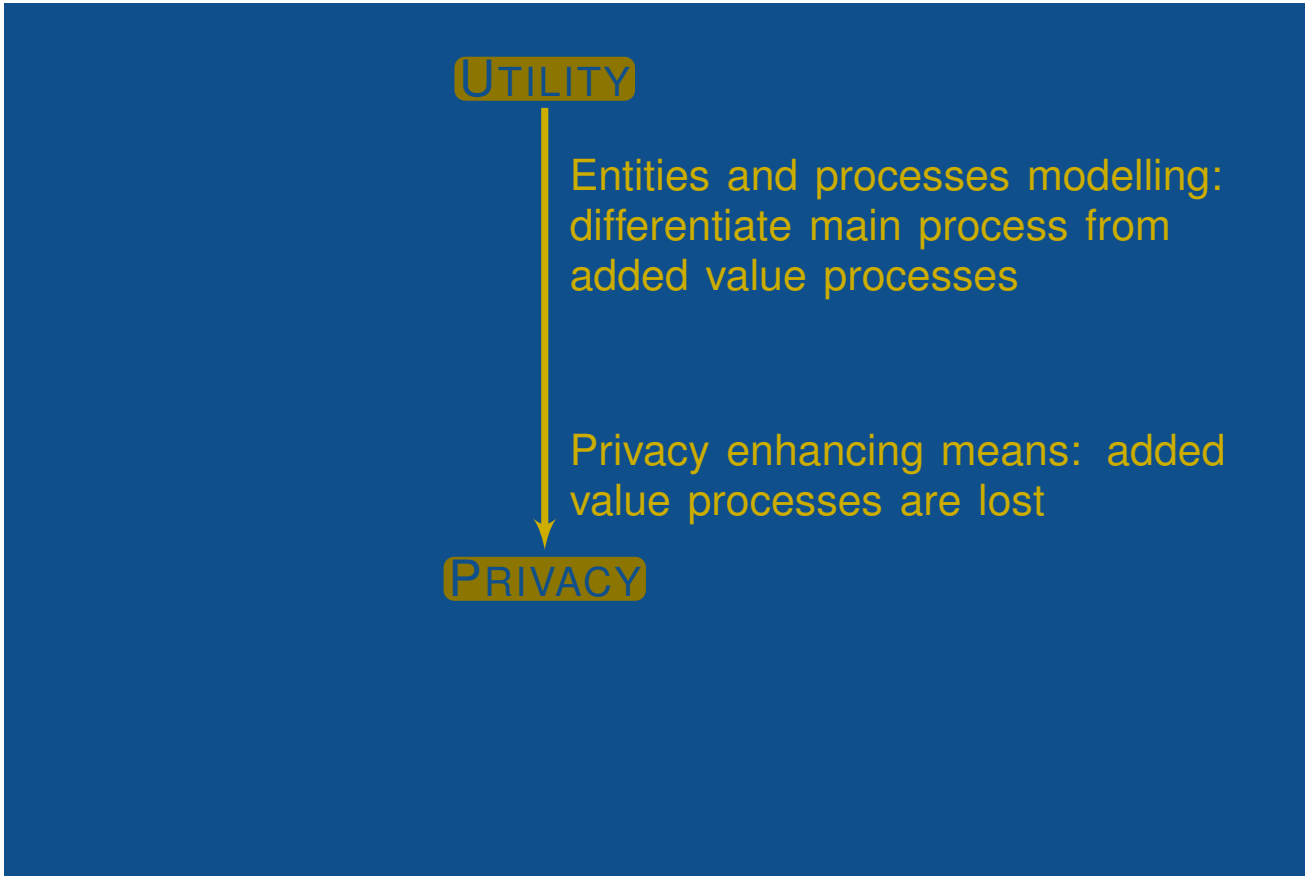
UTILITY

Methodology

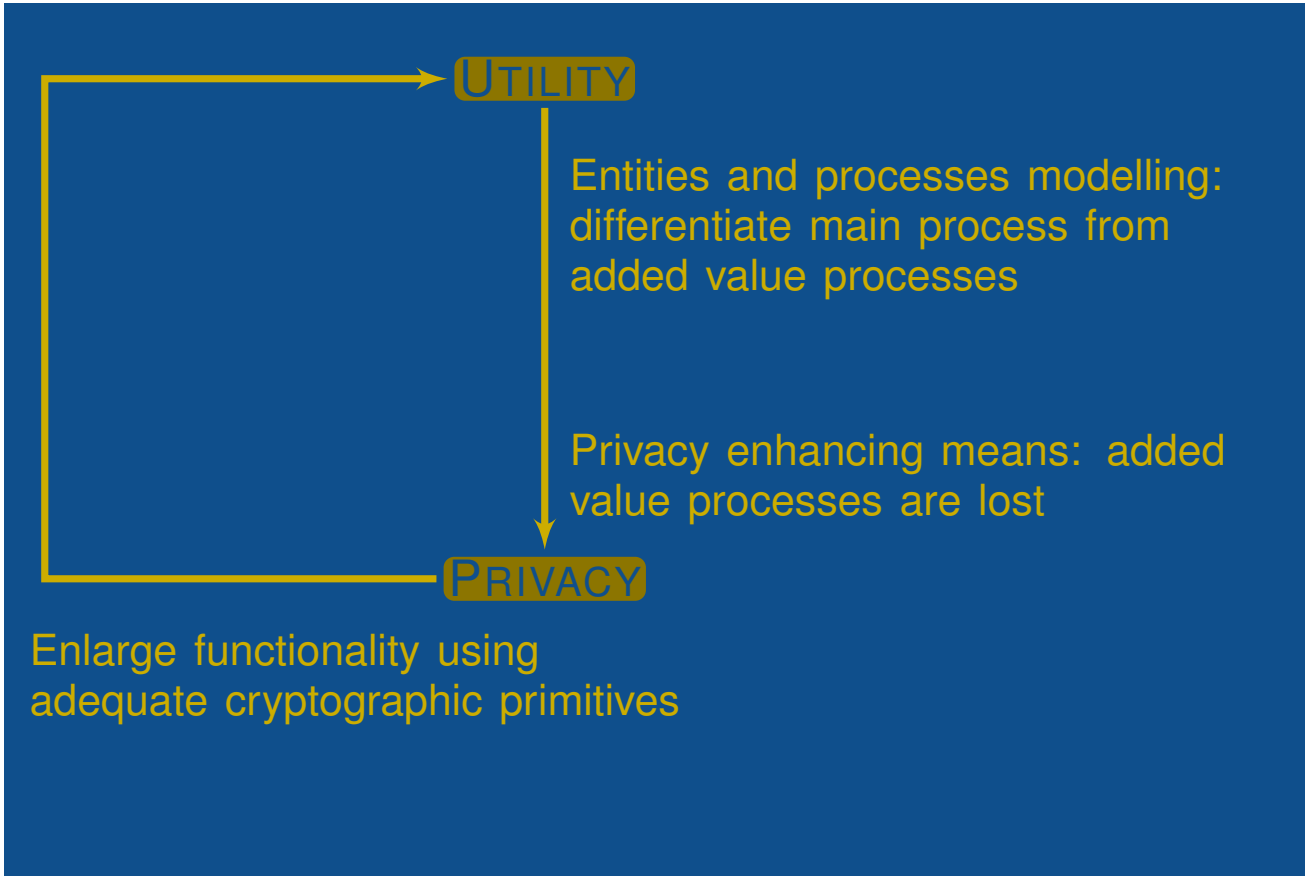
UTILITY

Entities and processes modelling: differentiate main process from added value processes

Methodology



Methodology



Basic cryptographic primitives

- ✓ Public-key encryption [DH76; RSA78]
  $(\texttt{EGen}, \texttt{Enc}, \texttt{Dec})$
- ✓ Digital signature
  $(\texttt{SGen}, \texttt{Sign}, \texttt{SVer})$
- ✓ commitment schemes [BCC88]
  $\mathsf{com}_m \leftarrow \mathsf{Com}(m; r_m)$, commitment to a message m
- ✓ Zero-knowledge proofs of knowledge (ZK-PoKs) [GMR89]
  $\pi \leftarrow \texttt{ProveZK}_L(x; w); \texttt{VerifyZK}_L(x, \pi)$

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

$\rho \leftarrow \texttt{GS.Sign}_{mk_i}(msg)$ issues a group signature ρ

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

$\rho \leftarrow \texttt{GS.Sign}_{mk_i}(msg)$ issues a group signature ρ

$\texttt{GS.Ver}_{pk_G}(\rho, msg)$ verifies whether ρ is a valid group signature

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

$\rho \leftarrow \texttt{GS.Sign}_{mk_i}(msg)$ issues a group signature ρ

$\texttt{GS.Ver}_{pk_G}(\rho, msg)$ verifies whether ρ is a valid group signature

$i \leftarrow \texttt{GS.Open}_{pk_G}(sk_G, \rho)$ returns the identity i having issued the signature ρ

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

$\rho \leftarrow \texttt{GS.Sign}_{mk_i}(msg)$ issues a group signature ρ

$\texttt{GS.Ver}_{pk_G}(\rho, msg)$ verifies whether ρ is a valid group signature

$i \leftarrow \texttt{GS.Open}_{pk_G}(sk_G, \rho)$ returns the identity i having issued the signature ρ

$\pi \leftarrow \texttt{GS.Claim}_{mk_i}(\rho)$ creates a claim π of the ownership of ρ

Group signatures

- Group signatures ρ provide anonymity [CH91; CL02; KTY04; LY12; LPY12]
  - some member of the group created ρ

$(pk_G, sk_G) \leftarrow \texttt{GS.Setup}(1^k)$ sets up a key pair; GM holds sk_G

$\langle mk_i, \ell' \rangle \leftarrow \texttt{GS.Join}(pk_G)[M(s_i)GM(\ell, sk_G)]$ allows member M with secret s_i to join group G, generating the private member key mk_i and updating the Group Membership List ℓ to ℓ'

$\rho \leftarrow \texttt{GS.Sign}_{mk_i}(msg)$ issues a group signature ρ

$\texttt{GS.Ver}_{pk_G}(\rho, msg)$ verifies whether ρ is a valid group signature

$i \leftarrow \texttt{GS.Open}_{pk_G}(sk_G, \rho)$ returns the identity i having issued the signature ρ

$\pi \leftarrow \texttt{GS.Claim}_{mk_i}(\rho)$ creates a claim π of the ownership of ρ

$\texttt{GS.ClaimVer}_{pk_G}(\pi, \rho)$ verifies if π is a valid claim over ρ

Traceable signatures

+ . . . fairness support in terms of tracing

$t_i \leftarrow \texttt{TS.Reveal}_{sk_G}(i)$. The GM outputs the tracing trapdoor of identity i

Traceable signatures

+ ... fairness support in terms of tracing

$t_i \leftarrow \texttt{TS.Reveal}_{sk_G}(i)$. The GM outputs the tracing trapdoor of identity i

$b \leftarrow \texttt{TS.Trace}(t_i, \rho)$. Given the tracing trapdoor t_i, this algorithm checks if ρ is issued by the identity i and outputs a boolean value b reflecting the check

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

$(\tilde{m}, \pi) \leftarrow \texttt{PBS.Blind}_{pk_S}(m, r)$. Run by a user U, it blinds the message m using a secret value r. It produces the blinded message $\tilde{m}$ and a correctness proof π of $\tilde{m}$

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

$(\tilde{m}, \pi) \leftarrow \texttt{PBS.Blind}_{pk_S}(m, r)$. Run by a user U, it blinds the message m using a secret value r. It produces the blinded message $\tilde{m}$ and a correctness proof π of $\tilde{m}$

$\tilde{\rho} \leftarrow \texttt{PBS.Sign}_{sk_S}(cm, \tilde{m}, \pi)$. Signer S verifies proof π and issues a partially blind signature $\tilde{\rho}$ on $(cm, \tilde{m})$, where cm is the common message

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

$(\tilde{m}, \pi) \leftarrow \texttt{PBS.Blind}_{pk_S}(m, r)$. Run by a user U, it blinds the message m using a secret value r. It produces the blinded message $\tilde{m}$ and a correctness proof π of $\tilde{m}$

$\tilde{\rho} \leftarrow \texttt{PBS.Sign}_{sk_S}(cm, \tilde{m}, \pi)$. Signer S verifies proof π and issues a partially blind signature $\tilde{\rho}$ on $(cm, \tilde{m})$, where cm is the common message

$\rho \leftarrow \texttt{PBS.Unblind}_{pk_S}(\tilde{\rho}, \tilde{m}, r)$. Run by the user U, who verifies $\tilde{\rho}$ and then uses the secret value r to produce a final partially blind signature ρ

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

$(\tilde{m}, \pi) \leftarrow \texttt{PBS.Blind}_{pk_S}(m, r)$. Run by a user U, it blinds the message m using a secret value r. It produces the blinded message $\tilde{m}$ and a correctness proof π of $\tilde{m}$

$\tilde{\rho} \leftarrow \texttt{PBS.Sign}_{sk_S}(cm, \tilde{m}, \pi)$. Signer S verifies proof π and issues a partially blind signature $\tilde{\rho}$ on $(cm, \tilde{m})$, where cm is the common message

$\rho \leftarrow \texttt{PBS.Unblind}_{pk_S}(\tilde{\rho}, \tilde{m}, r)$. Run by the user U, who verifies $\tilde{\rho}$ and then uses the secret value r to produce a final partially blind signature ρ

$\texttt{PBS.Ver}_{pk_S}(\rho, cm, m)$ checks if ρ is valid

Partially blind signatures

✓ A blind signature allows a user U to have a signer S blindly sign the user's message m [Cha82]

\+ a common public message is included in the final signature [AF96]

$(pk_S, sk_S) \leftarrow \texttt{PBS.KeyGen}(1^k)$ sets up a key pair

$(\tilde{m}, \pi) \leftarrow \texttt{PBS.Blind}_{pk_S}(m, r)$. Run by a user U, it blinds the message m using a secret value r. It produces the blinded message $\tilde{m}$ and a correctness proof π of $\tilde{m}$

$\tilde{\rho} \leftarrow \texttt{PBS.Sign}_{sk_S}(cm, \tilde{m}, \pi)$. Signer S verifies proof π and issues a partially blind signature $\tilde{\rho}$ on $(cm, \tilde{m})$, where cm is the common message

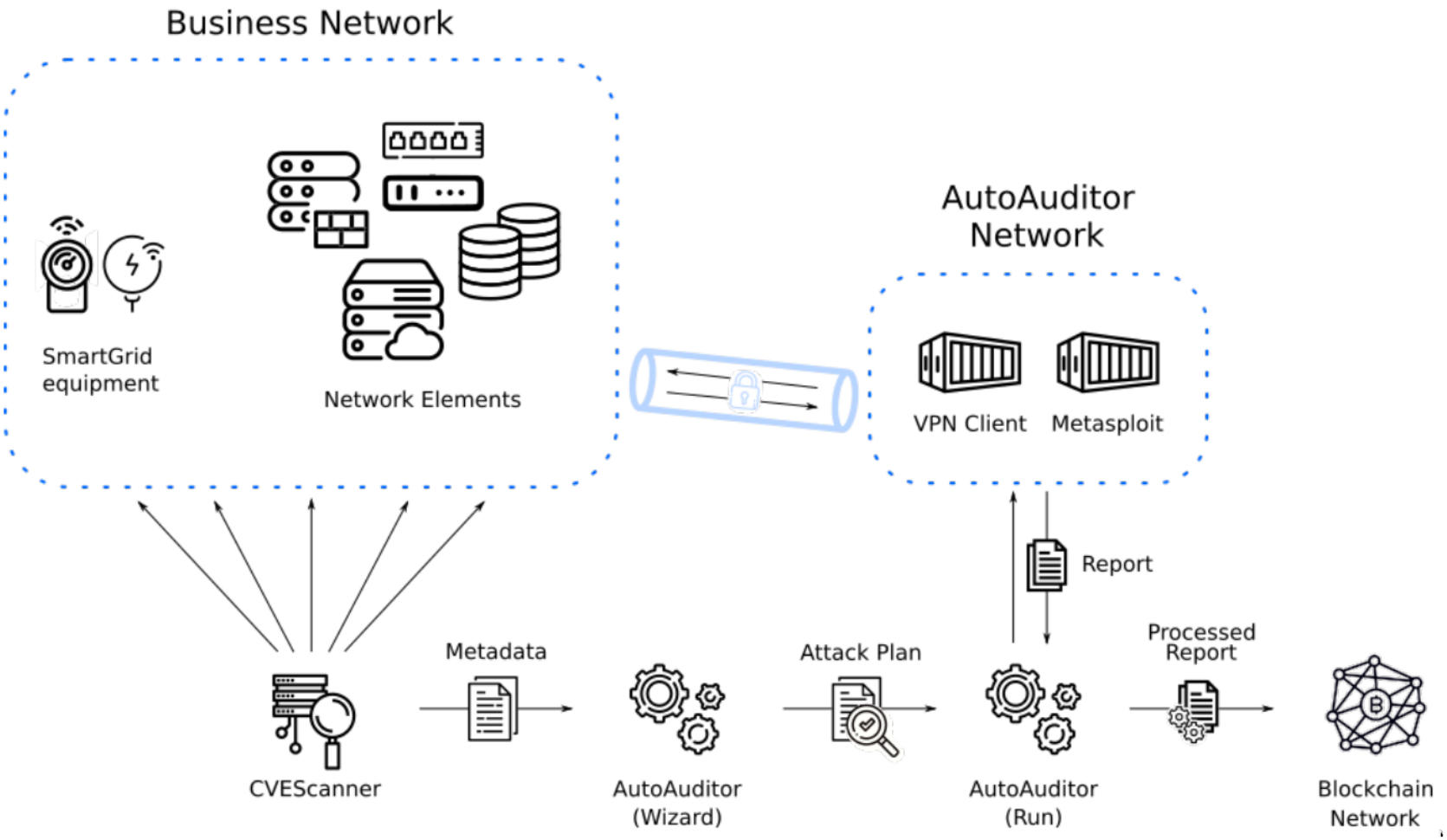
$\rho \leftarrow \texttt{PBS.Unblind}_{pk_S}(\tilde{\rho}, \tilde{m}, r)$. Run by the user U, who verifies $\tilde{\rho}$ and then uses the secret value r to produce a final partially blind signature ρ

$\texttt{PBS.Ver}_{pk_S}(\rho, cm, m)$ checks if ρ is valid

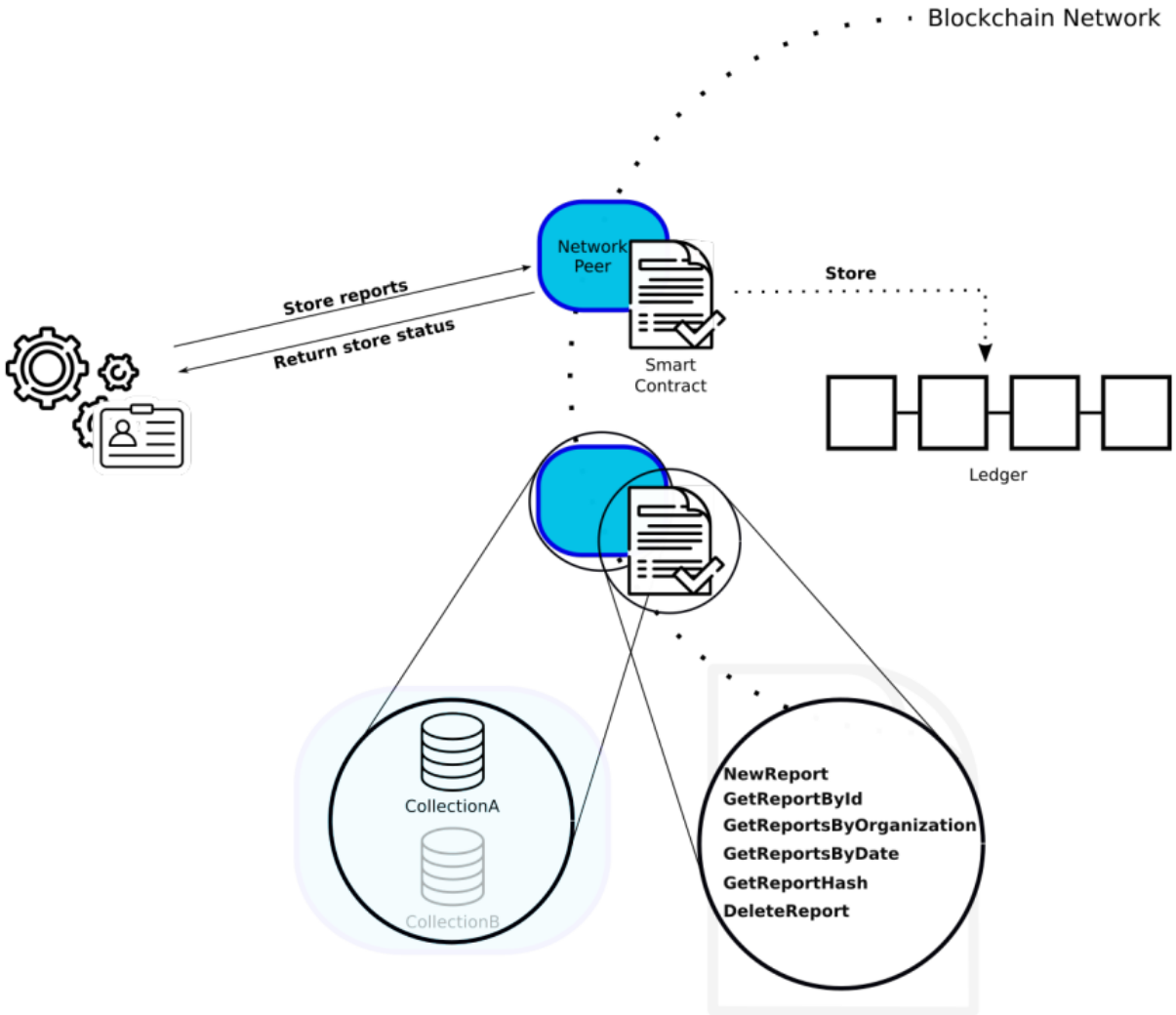
DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Sergio Chica y col. (2023). "Enhancing the anonymity and auditability of whistleblowers protection". En: *Blockchain and Applications, 4th International Congress*. Springer, págs. 413-422

AUTOAUDITOR architecture



AUTOAUDITOR workflow



https://gitlab.gast.it.uc3m.es/schica/autoauditor

Components

- **Whistleblowers:** Disclose confidential information in a totally anonymous way. They must have a valid group identity.

Components

- **Whistleblowers:** Disclose confidential information in a totally anonymous way. They must have a valid group identity.
- **Recipients:** Can decrypt and read disclosures anonymously addressed to them by Whistleblowers (1 to 1). Smart contract store certificate in the blockchain.

Components

- **Whistleblowers:** Disclose confidential information in a totally anonymous way. They must have a valid group identity.
- **Recipients:** Can decrypt and read disclosures anonymously addressed to them by Whistleblowers (1 to 1). Smart contract store certificate in the blockchain.
- **Verifier:** Permits the Whistleblowers retrieve a list of Recipients and published disclosures. Checks the validity of disclosures before publication: the signature of the disclosure must have been issued by a group member. The Verifier retrieves the public group key from the Provider.

Components

- **Whistleblowers:** Disclose confidential information in a totally anonymous way. They must have a valid group identity.
- **Recipients:** Can decrypt and read disclosures anonymously addressed to them by Whistleblowers (1 to 1). Smart contract store certificate in the blockchain.
- **Verifier:** Permits the Whistleblowers retrieve a list of Recipients and published disclosures. Checks the validity of disclosures before publication: the signature of the disclosure must have been issued by a group member. The Verifier retrieves the public group key from the Provider.
- **Provider (Issuer of group credentials):** Responsible of issuing group credentials to members of the fabric network, the potential whistleblowers, using a registration protocol.

Registration process: Recipients

- Who:
- What:
- How:

Registration process: Recipients

- Who: any member of the fabric network.
- What:
- How:

Registration process: Recipients

- Who: any member of the fabric network.
- What: receiving and decrypting anonymous disclosures.
- How:

Registration process: Recipients

- Who: any member of the fabric network.
- What: receiving and decrypting anonymous disclosures.
- How: storing the Recipient certificate in the blockchain granting Whistleblowers access to their certificate and be the target of disclosures.

Registration process: Whistleblowers

- Who:
- What:
- How:

Registration process: Whistleblowers

- Who: any member of the fabric network.
- What:
- How:

Registration process: Whistleblowers

- Who: any member of the fabric network.
- What: obtain group identity enabling to sign as a group member.
- How:

Registration process: Whistleblowers

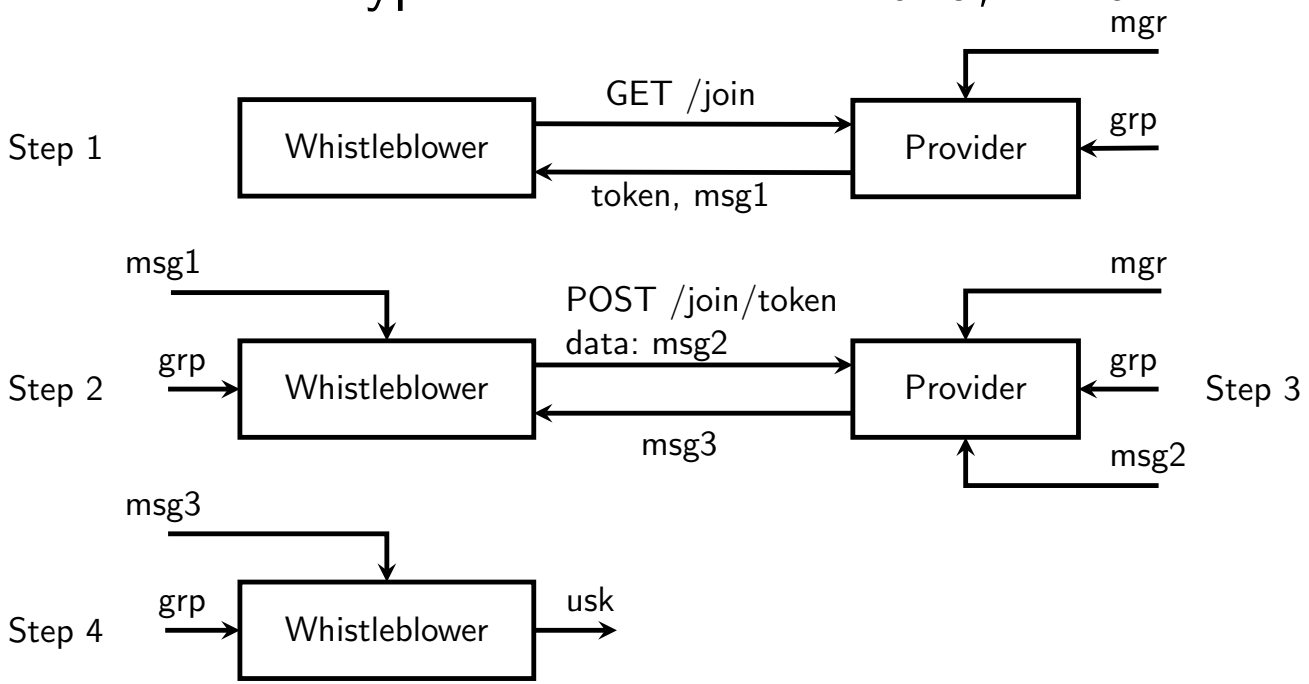
- Who: any member of the fabric network.
- What: obtain group identity enabling to sign as a group member.
- How: using the scheme PS16 implemented in libgroupsig

Diaz, J., Arroyo, D., Ortiz, F.: libgroupsig: An extensible c library for group signatures. IACR Cryptol. ePrint Arch. 2015, 1146.

Registration process: Whistleblowers

- Who: any member of the fabric network.
- What: obtain group identity enabling to sign as a group member.
- How: using the scheme PS16 implemented in libgroupsig

Diaz, J., Arroyo, D., Ortiz, F.: libgroupsig: An extensible c library for group signatures. IACR Cryptol. ePrint Arch. 2015, 1146.



Publication

- Whistleblower connects to Verifier (HTTPS).

Publication

- Whistleblower connects to Verifier (HTTPS).
- Whistleblower retrieves list of identifiers (registered Recipients).

Publication

- Whistleblower connects to Verifier (HTTPS).
- Whistleblower retrieves list of identifiers (registered Recipients).
- Whistleblower retrieves certificate of selected identifier.

Publication

- Whistleblower connects to Verifier (HTTPS).
- Whistleblower retrieves list of identifiers (registered Recipients).
- Whistleblower retrieves certificate of selected identifier.
- Whistleblower forgues an ephemeral key pair to send a message (envelope, content=encrypted disclosure, signature) to the verifier.

Publication

- Whistleblower connects to Verifier (HTTPS).
- Whistleblower retrieves list of identifiers (registered Recipients).
- Whistleblower retrieves certificate of selected identifier.
- Whistleblower forgues an ephemeral key pair to send a message (envelope, content=encrypted disclosure, signature) to the verifier.
- The message is stored in the blockchain.

Publication

- Whistleblower connects to Verifier (HTTPS).
- Whistleblower retrieves list of identifiers (registered Recipients).
- Whistleblower retrieves certificate of selected identifier.
- Whistleblower forgues an ephemeral key pair to send a message (envelope, content=encrypted disclosure, signature) to the verifier.
- The message is stored in the blockchain.
- Recipient may now retrieve the message and decrypt the disclosure.

Conclusions

- Anonymous disclosures in an open and auditable system.
- Confidential disclosures with forward secrecy using ECC SECP256R1.
- Public disclosures could be easily supported.
- Who can revoke whistleblower anonymity? PS16 vs DL21.
- group signatures guarantee the anonymity of Whistleblowers in their group.
- Anonymity: The Whistleblowers only needs to prove their identity when they join the group. Ulterior actions are not linkable to the registration process.
- Traceability: It is guaranteed that only those who have followed the registration process can generate valid group signatures.
- Non-frameability: it is not possible to create a group signature to incriminate another group member.

Future work

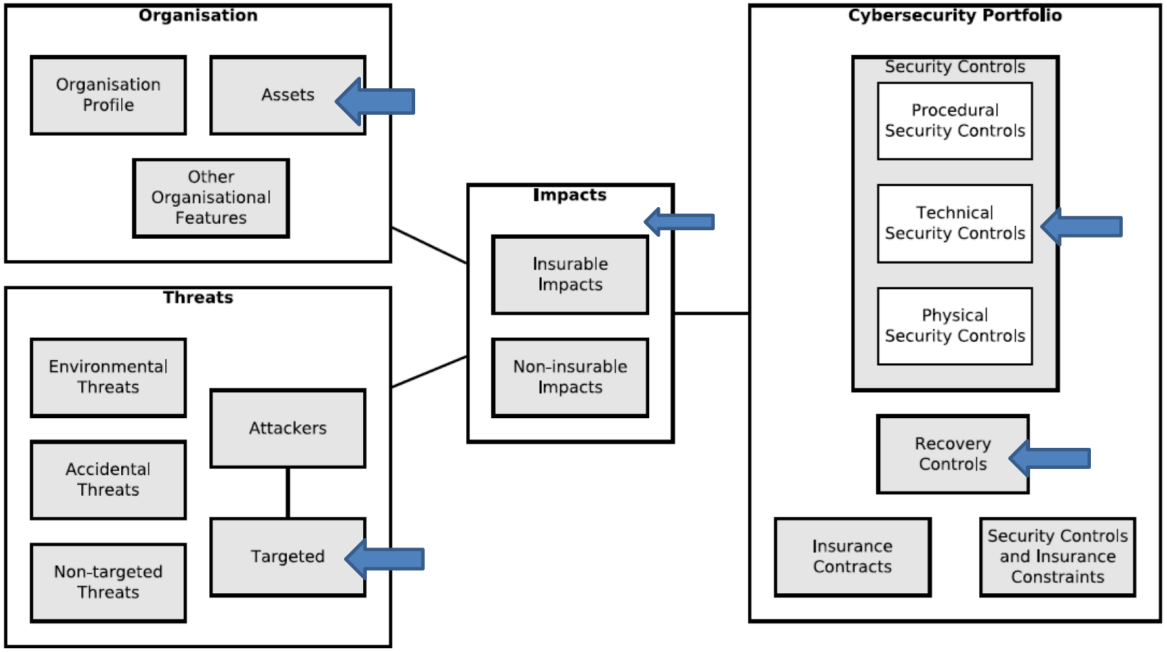
- Formalize registration and publication processes.
- Use external storage system like IPFS to alleviate the workload of the blockchain.
- Support future anonymous confidential communications between the Recipient and the Whistleblowers.
- Make a quantitative comparison with other proposals in the literature and release the code of the prototype.

Horizon2020
European Union Funding
for Research & Innovation

Grant agreement ID: 952622

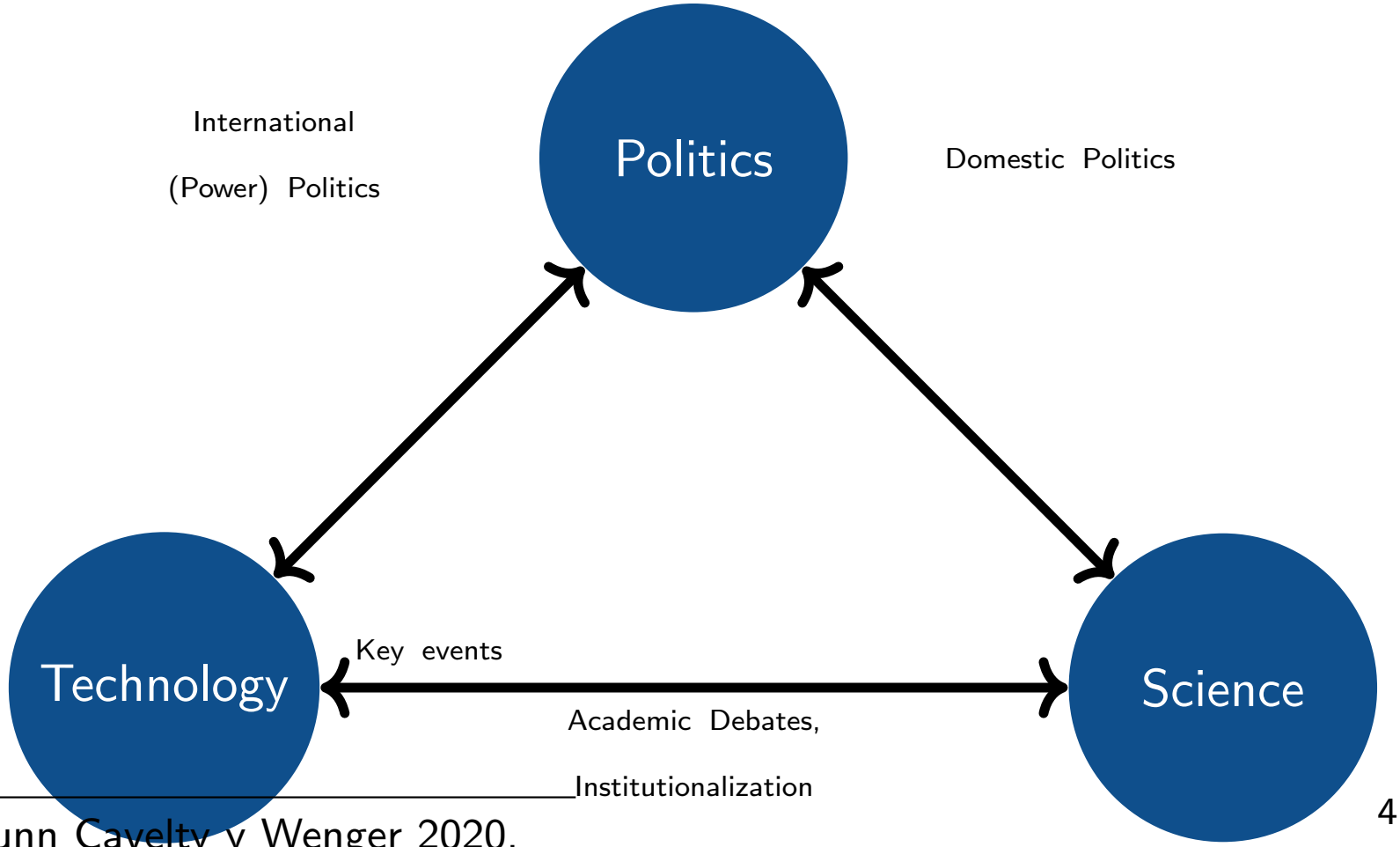
A risk management framework for systems with Artificial Intelligence components

- NIST Artificial Intelligence (AI) risk management framework
- The European Cyber- resilience Act
- The European Union AI Act


Organisation
Organisation Profile
Assets
Other Organisational Features
Threats
Environmental Threats
Accidental Threats
Non-targeted Threats
Attackers
Targeted
Impacts
Insurable Impacts
Non-insurable Impacts
Cybersecurity Portfolio
Security Controls
Procedural Security Controls
Technical Security Controls
Physical Security Controls
Recovery Controls
Insurance Contracts
Security Controls and Insurance Constraints

RISC-V Development foci from Architecture to Application

Latest policy developments on Open Source in the European Commission



[4] Dunn Cavelty y Wenger 2020.

GiCP's role in GOIT

WP4

- Identification of the most critical scientific and technical areas for promoting the culture of open-source in the deployment of secure hardware
- Survey of (semi-)automatic procedures to guide the analysis, design and audit of open-source hardware
- Study of the openness of the most relevant standardization bodies in security and safety
- Identification of the most relevant standardization committees for promoting a culture of open-source in dependable hardware and hardware in general

Roadmap

- Task 4.1. Identification of the main initiatives in the development of open source hardware (M1-M6)
- Task 4.2. Improvement of open hardware methodologies and procedures by leveraging on the results of the main (cyber)security, safety and sustainability standardization committees (M6-M35)
- Task 4.3. Exploring the inclusion of open-source hardware in the complex standards-laws-certifications in cybersecurity (M6-M35).
  - Regulation (EU) 526/2013 and Regulation (EU) 2019/881 (Cybersecurity Act)
  - Proposal for Cyber resilience Act-2022-09-15 (due time: November 14th)

WHAT

EU legislation: Council, EC, EP

- Public authority
- Mandatory
- Setting what goals to reach
- Revised when policy requires

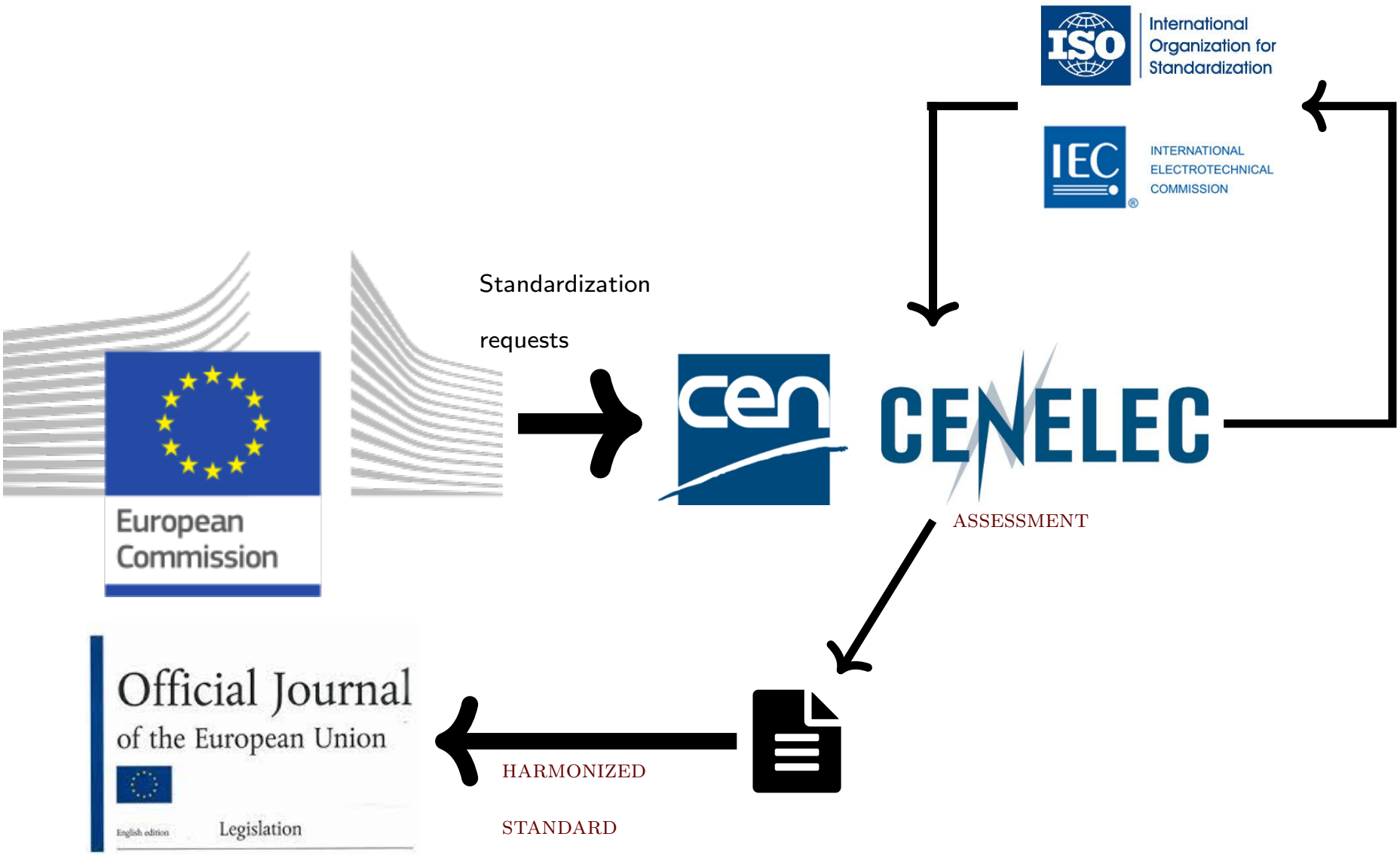
Requirements to protect public interest

HOW

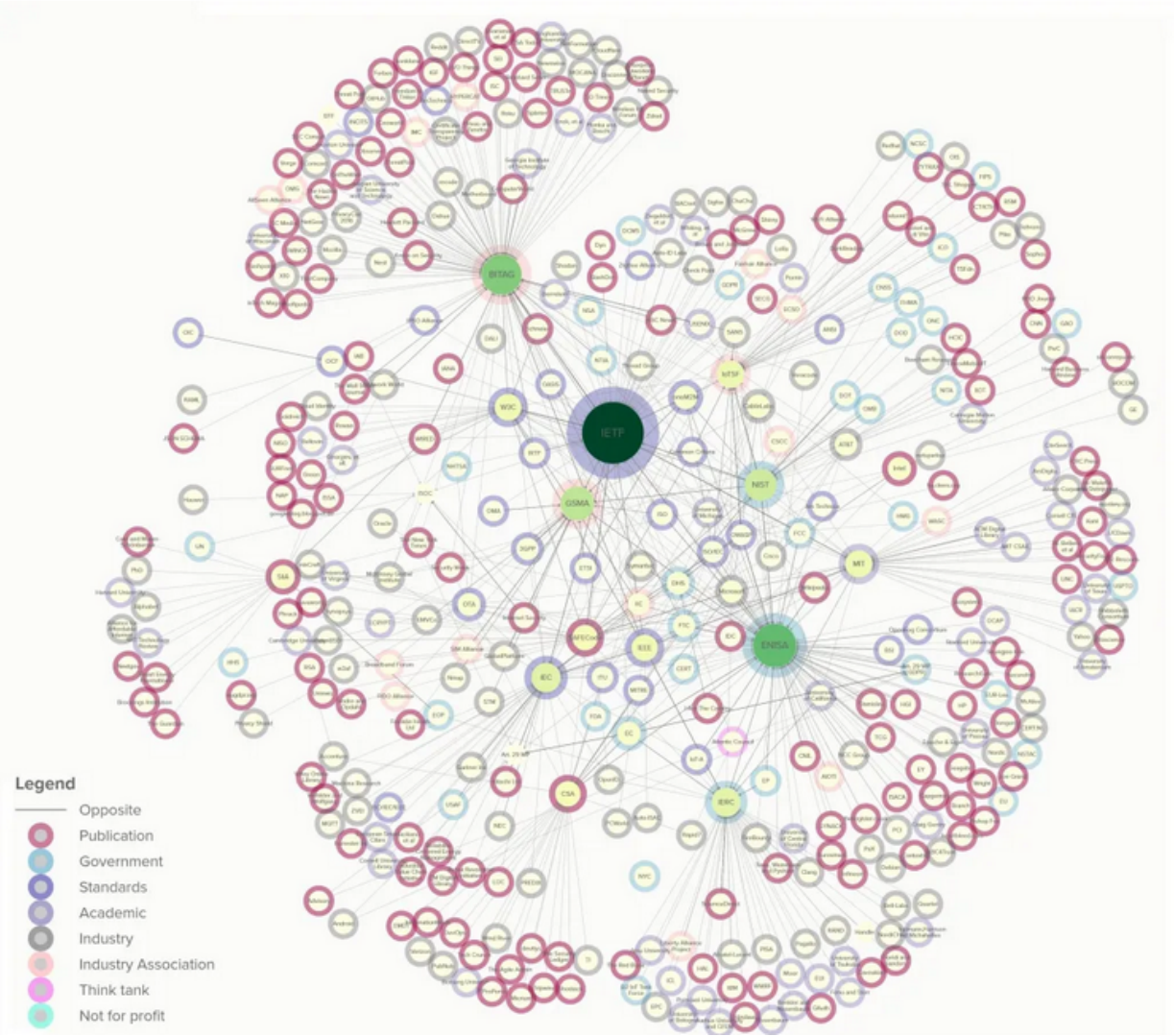
European Standards Organizations

- Private independent organizations
- Voluntary
- How to reach goals
- State of the art

Link with EU legislation and Standardization req



Mapping Security & Privacy in the Internet of Things



CEN-CLC/JTC 13 Strategy I

- Transponse all relevant standards to European Standards (EN) according to international agreements
  - ISO/IEC 270XXX family
  - Common Criteria ISO/IEC 15408/18045
  - Privacy Standards ISO/IEC 29100/29101/29134/27701
  - Vulnerability disclosure ISO/IEC 29147/30111
- Cooperation with ETSI
  - EN 303 645 "Cybersecurity for Consumer IoT"
- Liaise and cooperate with
  - Other European Organizations (ANEC, ECSO, SBS)
  - CEN-CLC TCs active in cybersecurity verticals
- Feasibility studies
  - PQC
  - Cybersecurity rating
  - Cybersecurity of AI

Spanish mirror Committee to CEN/CLC JTC13: UNE CTN320

- Develop technical standards to effectively respondo to cybersecurity challenges
- Information Security Management System (ISMS), IT product / IoT security, cloud security, ElectronicEvidence, Connected and Automated Mobility (CAM) security, etc.
- Standard UNE320001 Çybersecurity evaluation methodology LINCE for ICT products"(⇒ European standard EN17640)
- UNE320002 "Trusted architectures for the exchange of Cyber Threat Intelligence", UNE71510, UNE71512, and UNE71513 standards on applications with electronic National Identity Card (DNIe), and the creation and verification of electronic evidence

Eva Freund (2012). “IEEE standard for system and software verification and validation (IEEE Std 1012-2012)”. En: *Software quality professional* 15.1, pág. 43

Three pending workshops (GOIT)

- Report describing goals, communication strategy and target audience in the organization of workshops to promote the adoption of open hardware in standardization and certification initiatives [september 2023]
- Organization of a workshop on open source hardware and cybersecurity [september 2024]
- Organization of a workshop on open source hardware and artificial intelligence [december 2024]
- Organization of a workshop on open source hardware, digital forensics, audit and certification [abril 2025]

Funding

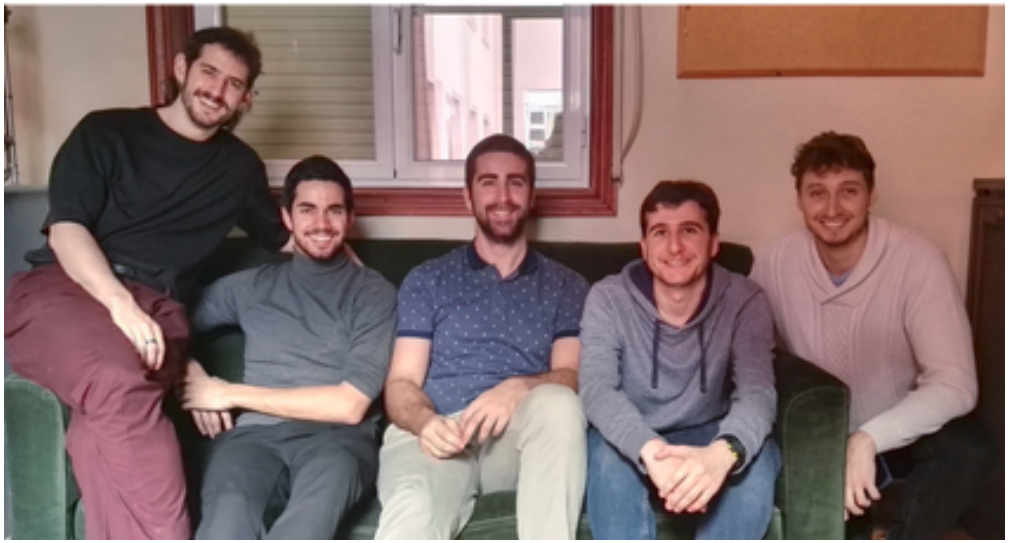
Grant Agreement No. 952622 under the EU H2020

Grant Agreement No. 101070660 under the EU HE

Grant Agreement No. 872855 under the EU H2020

Thanks to the team: they are the reason why...

Thanks to the team: they are the reason why...



+ Sergio de la Chica
+ Postdoc (along this month...)
+ ...

If you are interested in collaborating with us...

https://dargcsic.github.io/

References I

- Ahmad, Atif, Jeb Webb, Kevin C Desouza y James Boorman (2019). "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack". En: *Computers & Security* 86, págs. 402-418.
- Beaumont, Mark, Bradley Hopkins y Tristan Newby (2011). "Hardware Trojans-prevention, detection, countermeasures". En: *DSTO, defense science and technology organization, PO Box* 1500.
- Chica, Sergio, Andrés Marın, David Arroyo, Jesús Dıaz, Florina Almenares y Daniel Dıaz (2023). "Enhancing the anonymity and auditability of whistleblowers protection". En: *Blockchain and Applications, 4th International Congress*. Springer, págs. 413-422.
- Degli Esposti, Sara y Carles Sierra (2021). *White Paper on Artificial Intelligence, Robotics and Data Science*. Consejo Superior de Investigaciones Cientıficas (España).

References II

- Diaz, Jesus, David Arroyo y Francisco B Rodriguez (2014). "New x. 509-based mechanisms for fair anonymity management". En: *Computers & Security* 46, págs. 111-125.
- Diaz, Jesus, Seung Geol Choi, David Arroyo, Angelos D Keromytis, Francisco B Rodriguez y Moti Yung (2019). "A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions". En: *Advances in Cyber Security: Principles, Techniques, and Applications*. Springer, Singapore, págs. 143-183.
- Dunn Cavelty, Myriam y Andreas Wenger (2020). "Cyber security meets security politics: Complex technology, fragmented politics, and networked science". En: *Contemporary Security Policy* 41.1, págs. 5-32.
- Freund, Eva (2012). "IEEE standard for system and software verification and validation (IEEE Std 1012-2012)". En: *Software quality professional* 15.1, pág. 43.

References III

- He, Yingzhe, Guozhu Meng, Kai Chen, Xingbo Hu y Jinwen He (2019). "Towards privacy and security of deep learning systems: a survey". En: *arXiv e-prints*, arXiv-1911.
- Marın-López, Andrés, Sergio Chica-Manjarrez, David Arroyo, Florina Almenares-Mendoza y Daniel Dıaz-Sánchez (2020). "Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain". En: *Electronics* 9.11, pág. 1865.
- Osiceanu, Maria-Elena (2015). "Psychological Implications of Modern Technologies: "Technofobia" versus "Technophilia"". En: *Procedia - Social and Behavioral Sciences* 180. The 6th International Conference Edu World 2014 "Education Facing Contemporary World Issues", 7th - 9th November 2014, págs. 1137-1144. ISSN: 1877-0428.

References IV

- Torre-Abaitua, Gonzalo de la, Luis Fernando Lago-Fernández y David Arroyo (2021). "A Compression-Based Method for Detecting Anomalies in Textual Data". En: *Entropy* 23.5, pág. 618.
- Van Goethem, Tom, Christina Pöpper, Wouter Joosen y Mathy Vanhoef (2020). "Timeless timing attacks: Exploiting concurrency to leak secrets over remote connections". En: *29th {USENIX} Security Symposium ({USENIX} Security 20)*, págs. 1985-2002.