THE UNIVERSITY of EDINBURGH

Cyber Security, Privacy and Trust PhD Programme

Prof. David Aspinall (Programme Director), Dr. Daniel Woods (Selector)

13th November 2024. See https://web.inf.ed.ac.uk/security-privacy/phd-study

EDINBURGH
xtraordinary futures await

UoE Cyber Security, Privacy and Trust Research

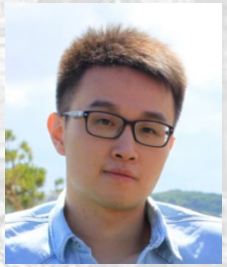
- >20 academics, about 30 post-doc researchers, 25 PhDs
- **Informatics SPT** Group plus links with other departments
- UoE is a UK Gov-recognised centre of excellence for research (ACE-CSR)
- In top 5 in EU for cyber research (csrankings.org).

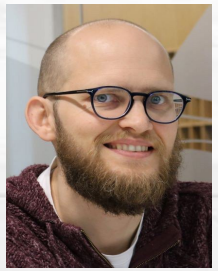
Our approach:

- Breadth: **multi-disciplinary collaborations**
- Research style: **fundamental**, foundations with applications
- Reach: Scotland, UK, **international**

National Cyber Security Centre

Academic Centre of Excellence in Cyber Security Research



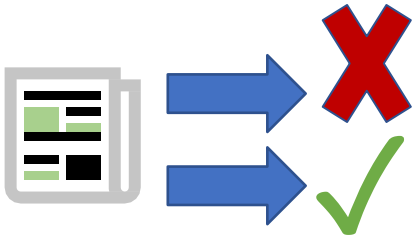


EDINBURGH
CYBER SECURITY
PRIVACY & TRUST
INSTITUTE

Security, privacy, and trust are problems that cut across nearly all aspects of how we interact with computers

Cyber Privacy

Privacy



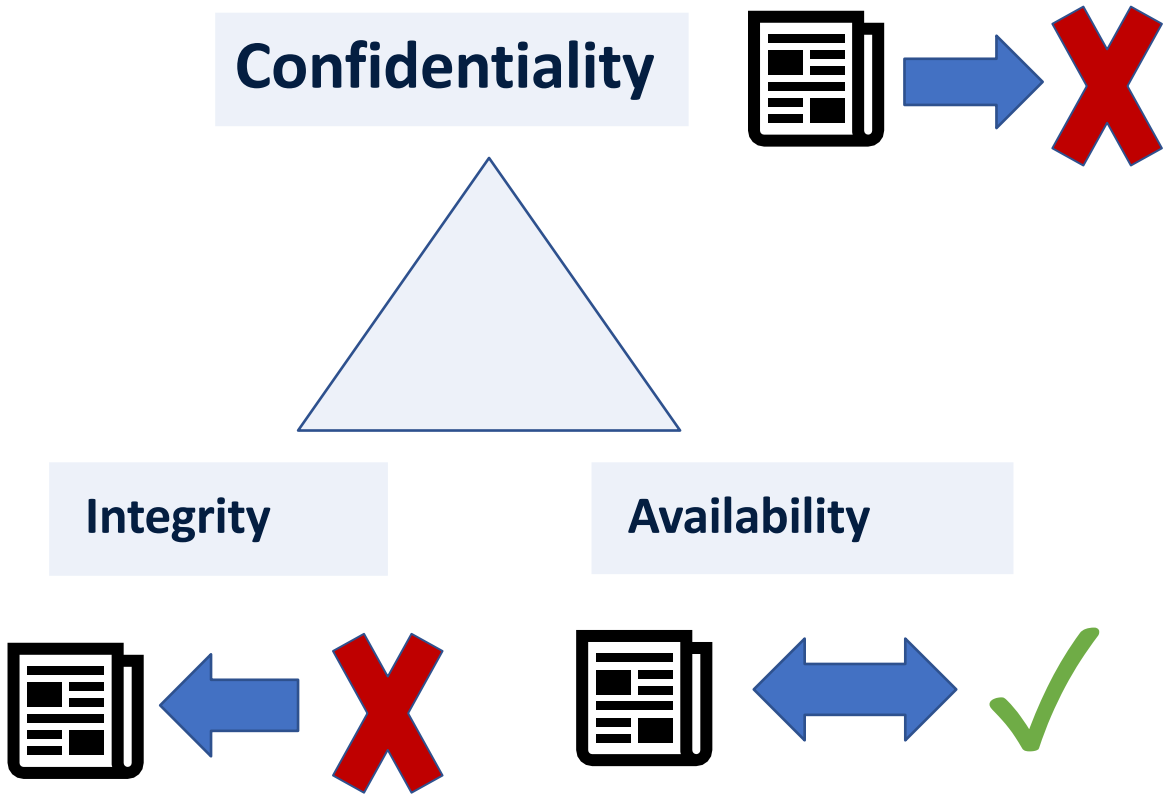
Privacy is about *partial* sharing of information between parties.

Often (but not necessarily) concerns **personal** information.

Attacker may be a legitimate recipient.

PETs, *Privacy Enhancing Technologies* are emerging methods to handle this.

Cyber Security



The traditional “CIA Triad”:

- **C** - no unauthorized information access
- **I -** no unauthorized data alteration
- **A -** services appropriately accessible

Cyber Trust

Authorization assumes notions of **identity** and **trust**.

Blockchain and ledgers provide new solutions to entity trust and consensus.

Verification and attestation provide solutions to system trust.

Some of our research themes

- **AI** and Security
- **Data Science** and Security **Distributed**
- **Blockchain and Distributed Ledger**
- **Cryptography**
- Secure Future **Networks**
- Privacy and Security on **Hardware Devices**
- **Security and Reliability** in systems
- Protocol and Program **Verification**
- **Quantum** Cyber Security
- **Socio-technical**, **Human Factors**, **Law, Risk**

PhD in CSPT: What is it?

A PhD trains you as an **academic researcher**

- Develop an **all-round knowledge** of the discipline
- Develop advanced techniques and **in-depth knowledge in a specialist area of cyber security, privacy and trust**
- Acquire a broad range of **transferable skills**

One overriding requirement: a passion for your research topic!

PhD in CSPT: What will you do?

- Carry out **independent research**
- Produce **original contributions** to knowledge in your chosen area
  - writing and publishing academic papers
  - presenting your work at workshops, conferences
- Work under the **guidance of your supervisors**
- Sometimes: work with an industry partner, undertake internships

PhD in CSPT: Final Outcome

- Submit a **PhD thesis**
- Defend your thesis in an **oral examination**
- Assessed according to UoE **assessment regulations**
  - PhD: a **new and significant** contribution to knowledge
- Get awarded a **doctoral degree**
- Then... go on to your next career stage: **academic or industry researcher, engineer, entrepreneur, cyber security visionary...**

PhD in CSPT: First Year

- **Probationary**
- Develop **literature review** and a **thesis proposal**
- Work with supervisor to identify **training needs**
- **Attend meetings** relevant to your research topic
  - research seminars, group meetings and events
  - courses: graduate lectures, summer schools

PhD in CSPT: Progress through degree

- Assessed by **annual reviews**
- Determine whether you can progress to next year
- Thesis submission at the end of the third year (roughly)
- Followed by an oral examination
- Further information on of a PhD at UoE:
  http://edin.ac/2FBPNaw. **(PhD Code of Practice)**

PhD in CSPT: How to Apply

1. **Choose a topic** (at least area, need not be final/exact)
   - http://web.inf.ed.ac.uk/security-privacy/phd-study/ (guidance; example topics linked from this page)
2. Contact a **potential supervisor**
   - write a **research proposal** to discuss (topic, research idea, plan)
   - get agreement to **name potential supervisor** on the application
   - consider **funding** possibilities
3. **Apply** via the UoE web-site (needs degree certs, research proposal, etc)
   - https://www.ed.ac.uk/studying/postgraduate/degrees/

PhD in CSPT: Funding sources

You need money for fees and stipend (living costs). Fees depend on domicile.

Sources of funding:

1. **Funded PhD projects**

- available from some supervisors, usually tied to specific research

2. **UK Centres for Doctoral Training (CDTs)** programmes on related topics

- not CSPT programme; 4yrs and different application processes!
- see https://informatics.ed.ac.uk/study-with-us/our-degrees/postgraduate-research-and-cdts/centres-doctoral-training-cdts

THE UNIVERSITY of EDINBURGH

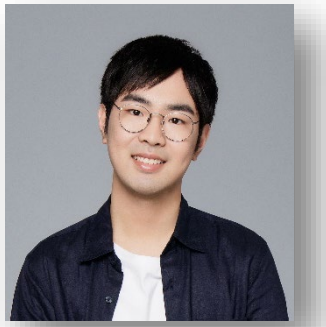
CSPT PhD : some research areas and previous research

EDINBURGH
xtraordinary futures await

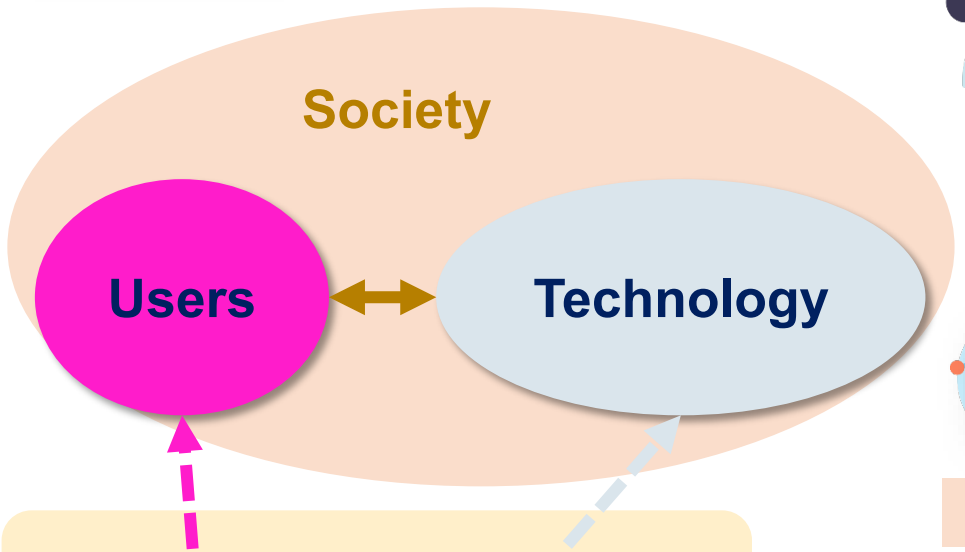
Human Factors

How to support people who make security and privacy work.

User-Centric Privacy and Security



Jingjie Li
Lecturer @ School of Informatics
Fully funded PhD studentship available for 2024
Website: www.jingjieli.me
Contact: jingjie.li@ed.ac.uk



Available Projects

Privacy-preserving interactive technologies

Interactive technologies in smart homes, augmented and virtual reality (AR/VR) accompany unprecedented privacy risks to consumers. We will understand the privacy requirements and design practical privacy enforcement for them.

Safety of interactive artificial intelligence (AI) agents

We are living in a world with more embodied and human-like AI agents that can make decisions and take action, despite their rising safety concerns. We will evaluate the safety issues of interactive AI agents and develop mechanisms to address these gaps.

Internet culture of privacy and security

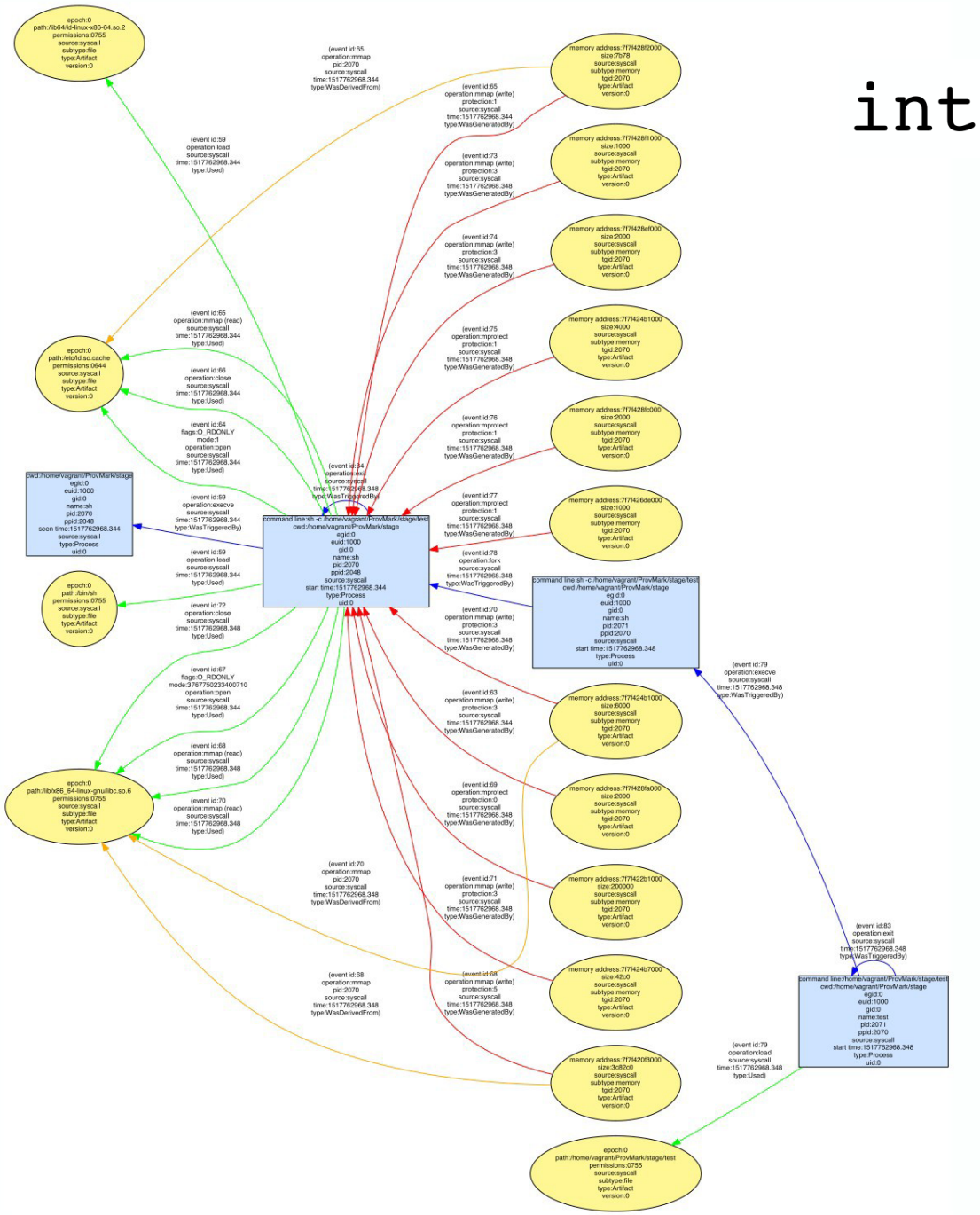
Privacy and security have become cultural phenomena on the Internet and influence people's behaviors. We will study the interplay between cultures and people's privacy and security behaviors through online communities.

Preferred Experiences

Privacy and security research; User/HCI studies; AI (particularly language models); Software/hardware design and prototyping; Internet measurement

Trust: Data, Origin, Provenance

Knowing and controlling where “stuff” come from and being certain of that data’s accuracy.



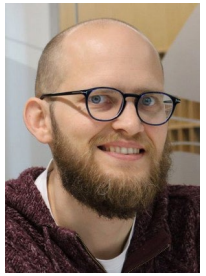
```
int main () {return 0;}
```

Programming-language oriented security.

Wide-range tracking of data, computing

Applications: supply chain, forensics

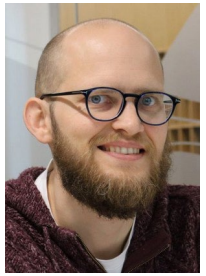
Digital traceability and value flow



design informatics

INPUT | OUTPUT

Making transaction choices manifest



design informatics

INPUT | OUTPUT

Verification and Modelling

How do we know for certain that the technologies we create are “secure”?

Protocol and Program Verification

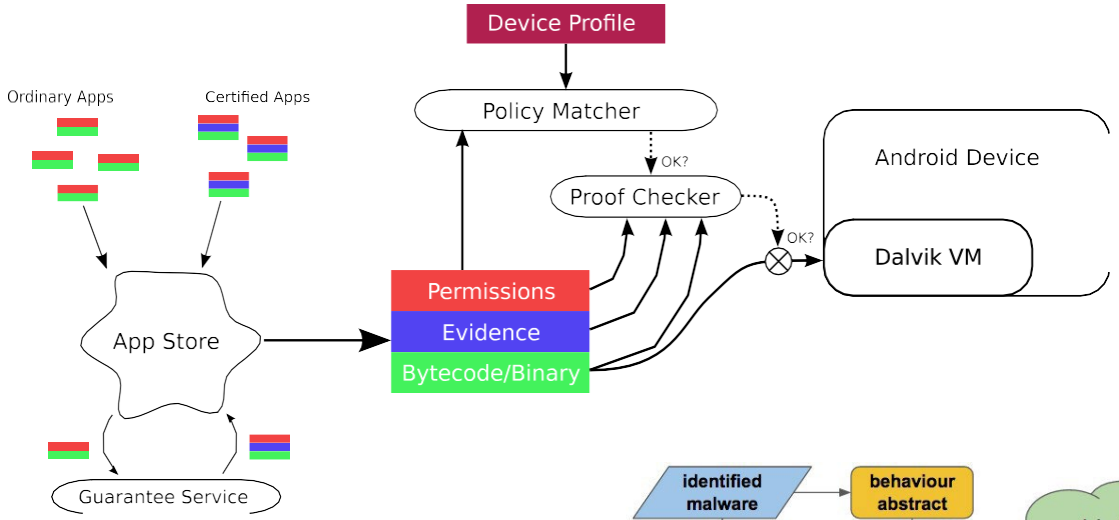
Foundations

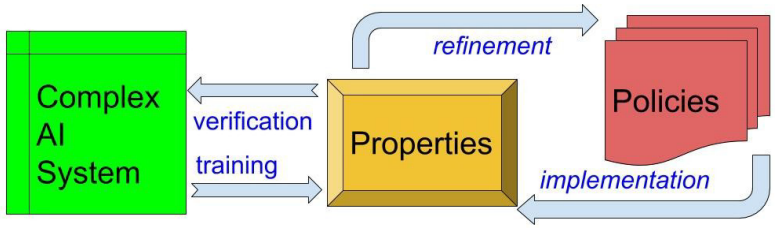
- Formal logics and programming languages
- Protocol design analysis
- Verified cryptographic proofs

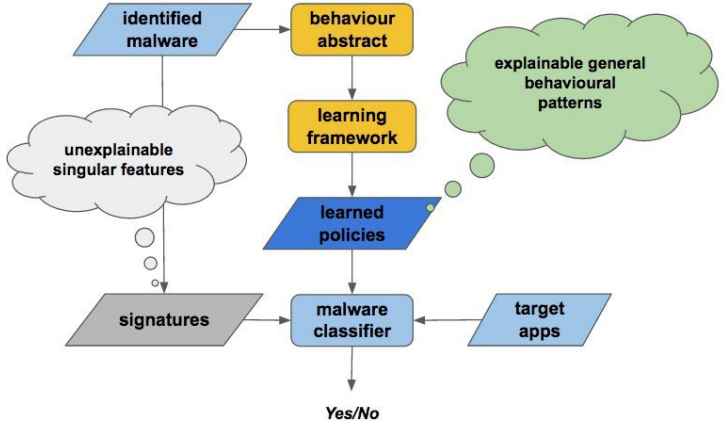
Applications

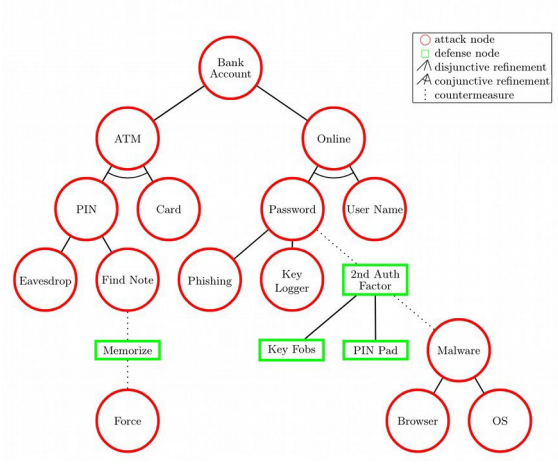
- Checking software implementations
- Discovering and fixing flawed designs

Cyber Security Modelling and Verification

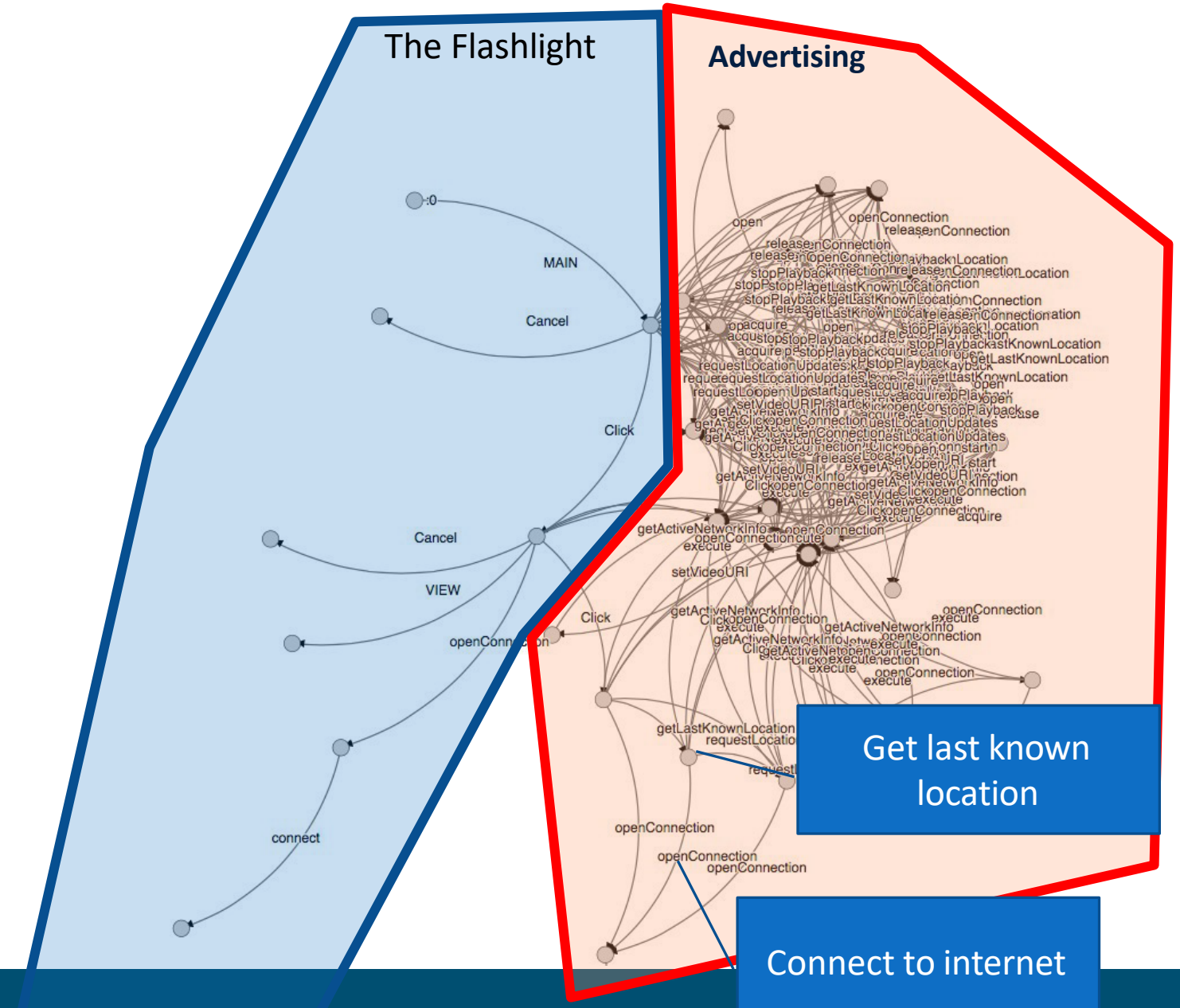








Security static analysis: Break an app up into a flow diagram



Quantum Cyber Security

Quantum cloud computing

- Hybrid quantum-classical server-client
- Infrastructure: verification, quantum digital signatures

New applications

- Post-quantum cryptography
- Quantum blockchain
- Multi-party quantum computation

NOTE: See Quantum

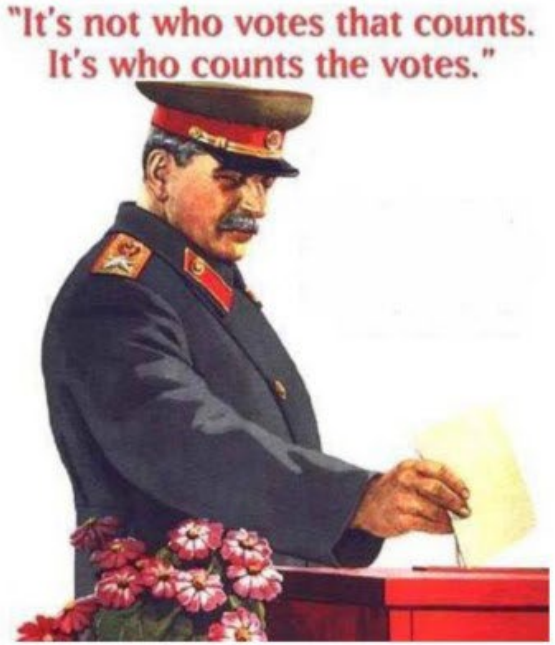
Electronic voting (e-voting)

Better efficiency

higher voter participation

greater accuracy

lower costs



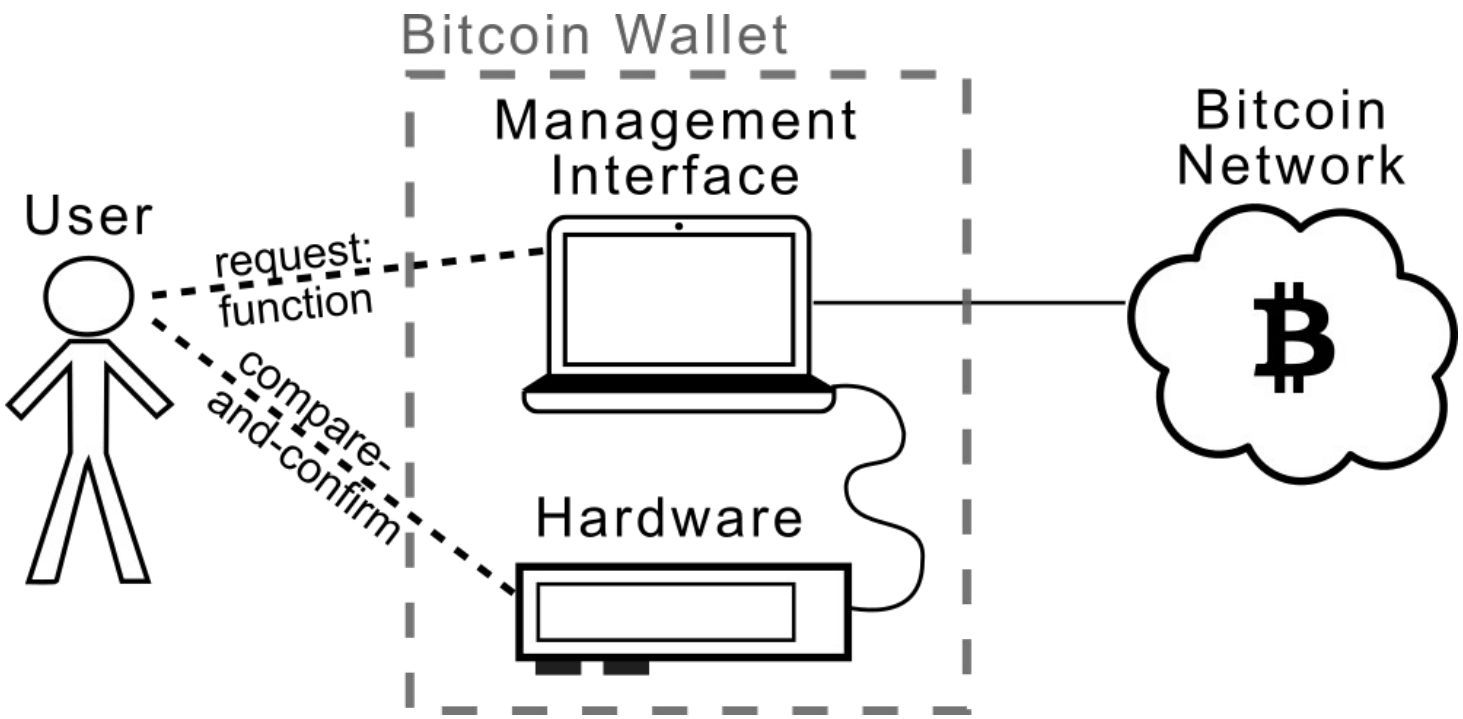
Better security

vote-privacy and voter-verification

even in the presence of

corrupt election authorities

Verifying the security of Bitcoin Hardware Wallets



Privacy Enhancing Technologies

How do we enable people, organizations and even governments protect their privacy?

Data Linkage: Combining data to learn new information

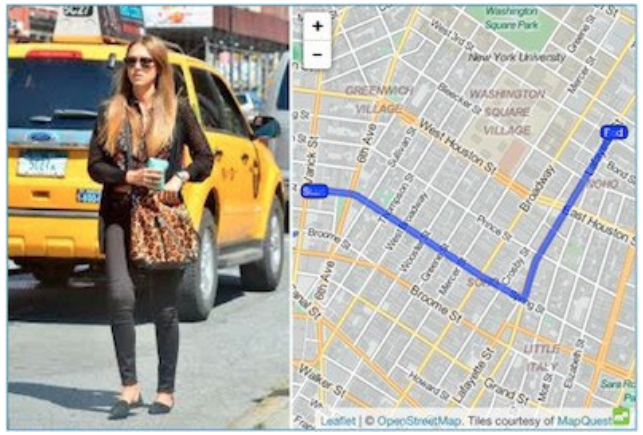
NETFLIX

IMDb

2007: Netflix releases viewing data recommender challenge.

Researchers de-anonymize entries,correlating with Internet Movie Database.

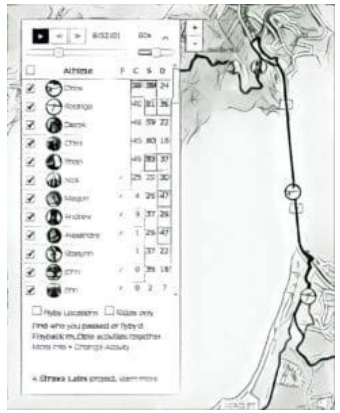
Revealed private watching habits.



2014: New York City Taxi dataset released to study traffic patterns, congestion.

Flawed anonymization, revealed driver identities. Incomes calculated.

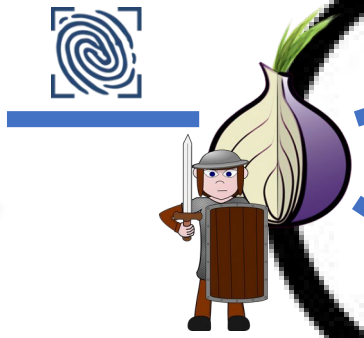
Paparazzi pics: celebrity journeys, homes, offices.

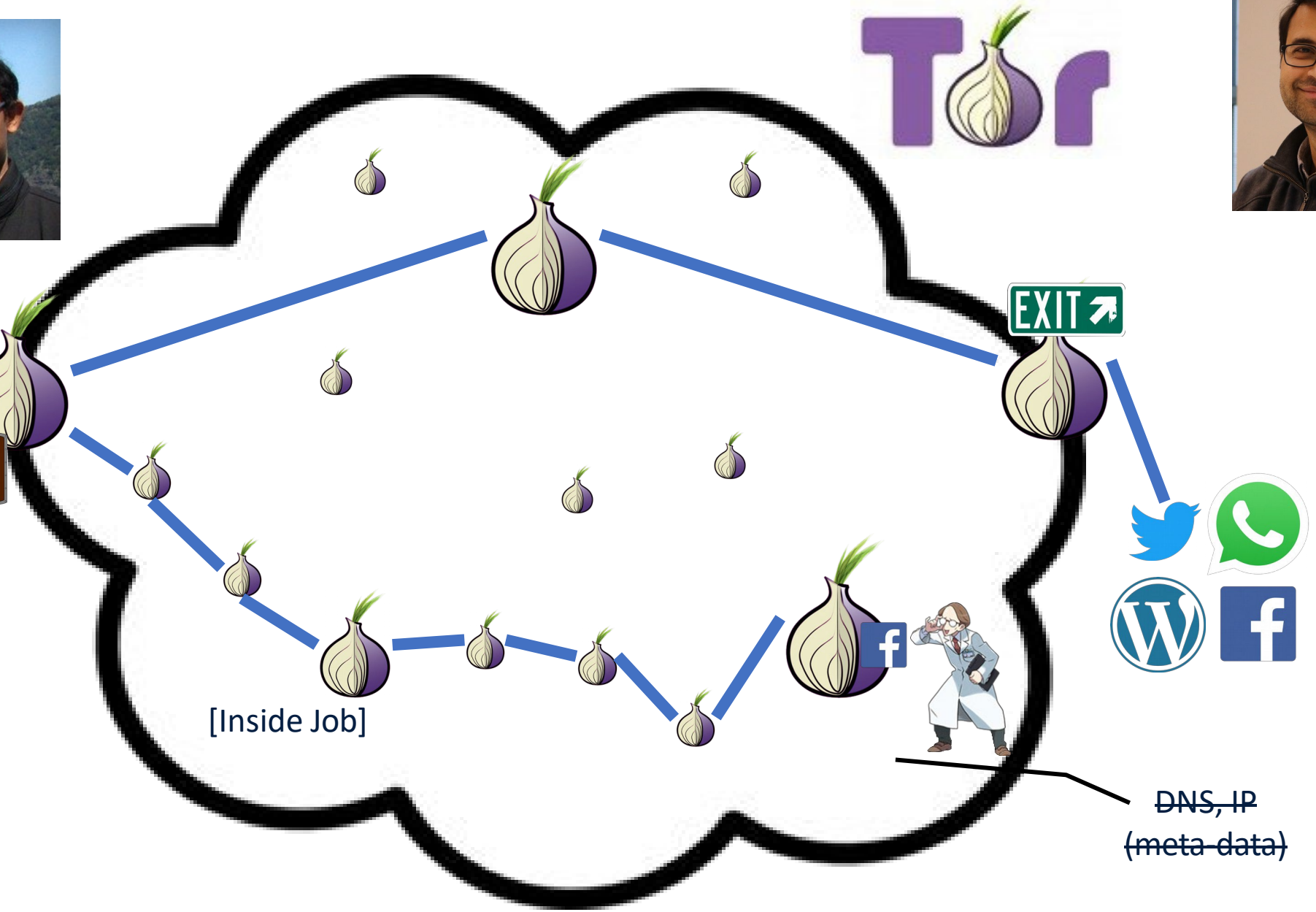


fitbit

2018: Strava heatmaps exposed military training locations and patterns.

Correlations with GPS-tagged photos, social media.

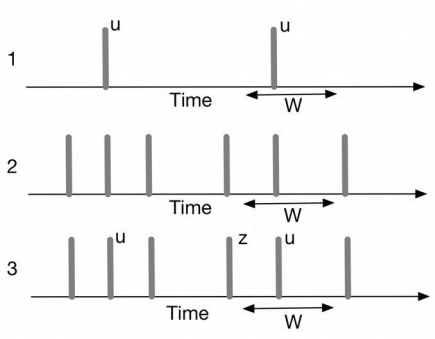


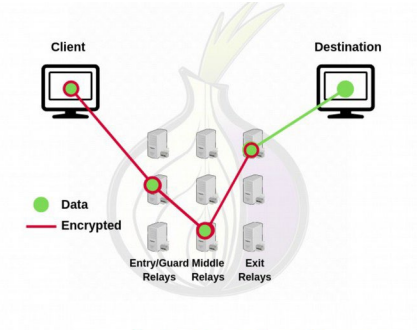


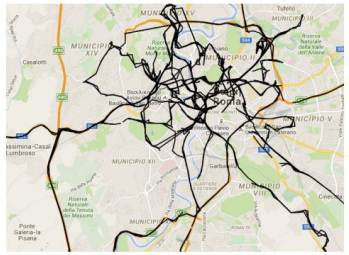
[Inside Job] Jansen R, Juarez M, Galvez R, **Elahi T**, Diaz C. Inside Job: Applying Traffic Analysis to Measure Tor from Within. Proceedings of the Network and Distributed System Security 2018. ISOC. 2018

Statistical Privacy

- Privacy of time and location
- Private queries on planar graphs
- Location anonymity through clustering
- Differentially private measurements in anonymity networks
- New privacy definitions
  - Privacy of correlated data
  - Privacy in infinite domains
- Privacy enhancement properties of ML techniques
- Private data summarization for ML







AI for Privacy, Responsible AI

- Detection of privacy violations in online systems (social networks,IoT systems)
- Prevention of privacy violations in online systems
- Context-based privacy in online systems
- Development of PETs to preserve privacy online

Blockchain and Distributed Ledger

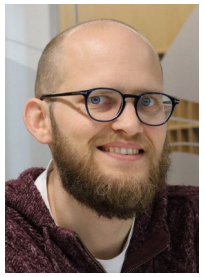
BLOCKCHAIN TECHNOLOGY LAB

Foundations

- Cryptographic properties of distributed ledgers
- Future distributed, cloud crypto: MPC, HE

Practice

- Blockchain Technology Laboratory IOHK
- Practical mix-nets, e-voting



Hardware and Networks

Making sure underlying technologies provide a strong base

AI for Security, Security of AI

National Cyber Security Centre

ABOUT NCSC | CISP | REPORT AN INCIDENT | CONTACT US

Home | Information for... | Advice & guidance | Education & skills | Products & services | News, blogs, events...

Home > Intelligent security tools

GUIDANCE

Intelligent security tools

Assessing intelligent tools for cyber security

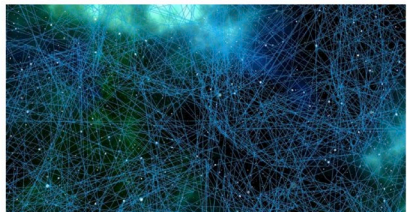
IN THIS GUIDANCE

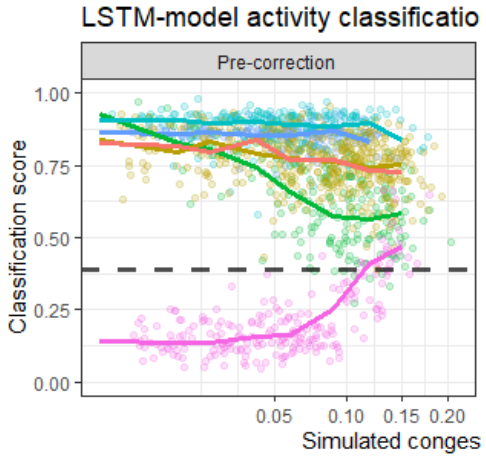
- Intelligent security tools
- Defining artificial intelligence
- Establishing the need
- Dealing with data
- Available skills and resources
- Getting the most from artificial intelligence

PUBLISHED
18 April 2019

REVIEWED
18 April 2019

VERSION
1.0



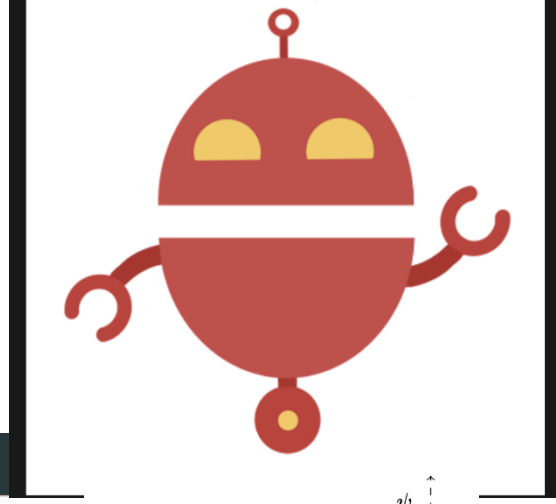


Bad Data Design Smells

Highly Repetitive
- Low Data Diversity
- Traffic Collapse

Simulation Artefacts
- Highly Dependent Features
- Artificial Diversity

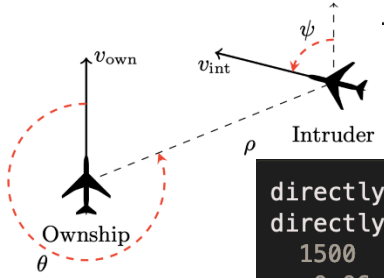
Mislabelled
- Wrong Label
- Unclear Ground Truth



Welcome to AISEC!

AI Secure and Explainable by Construction

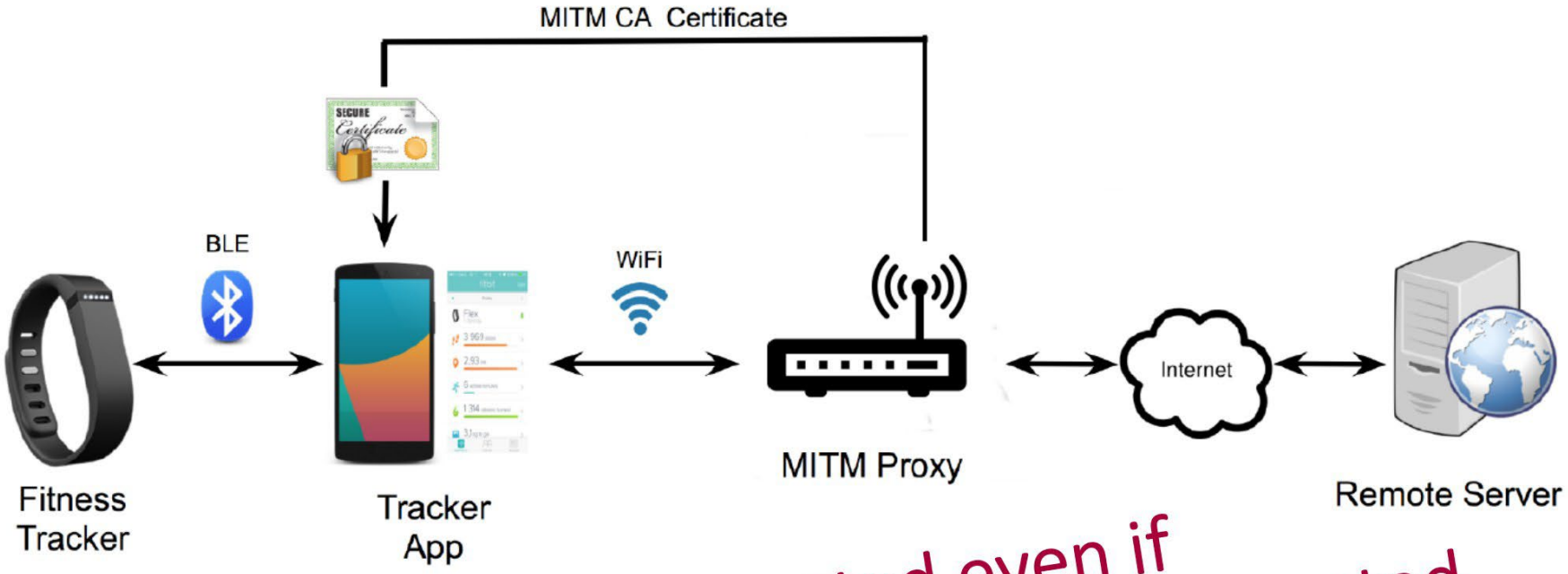
AI applications have become pervasive: from mobile phones and home appliances to stock markets, autonomous cars, robots, and drones. Each application domain comes with a rich set of requirements such as legal policies, safety and security standards, company values, or simply public perception. **The AISEC** project aims to build a sustainable, general purpose, and multidomain methodology and development environment for policy-to-property secure and explainable by construction development of complex AI systems.




```
directlyAhead : UnnormalisedInputVector -> Bool
directlyAhead x =
  1500  <= x ! distanceToIntruder <= 1800 and
  -0.06 <= x ! angleToIntruder    <= 0.06

movingTowards : UnnormalisedInputVector -> Bool
movingTowards x =
  x ! intruderHeading >= 3.10  and
  x ! speed           >= 980   and
  x ! intruderSpeed   >= 960
```

Can we make sense of the messages exchanged?

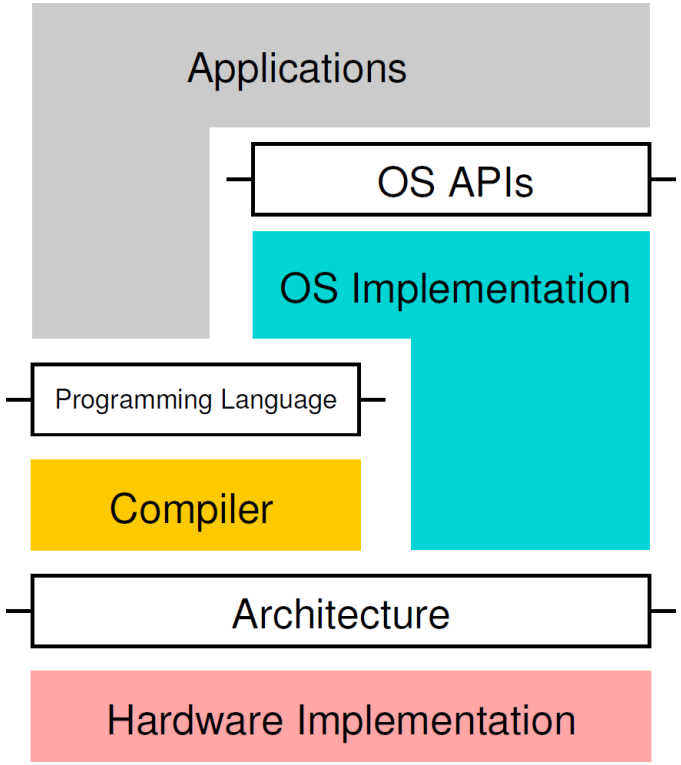


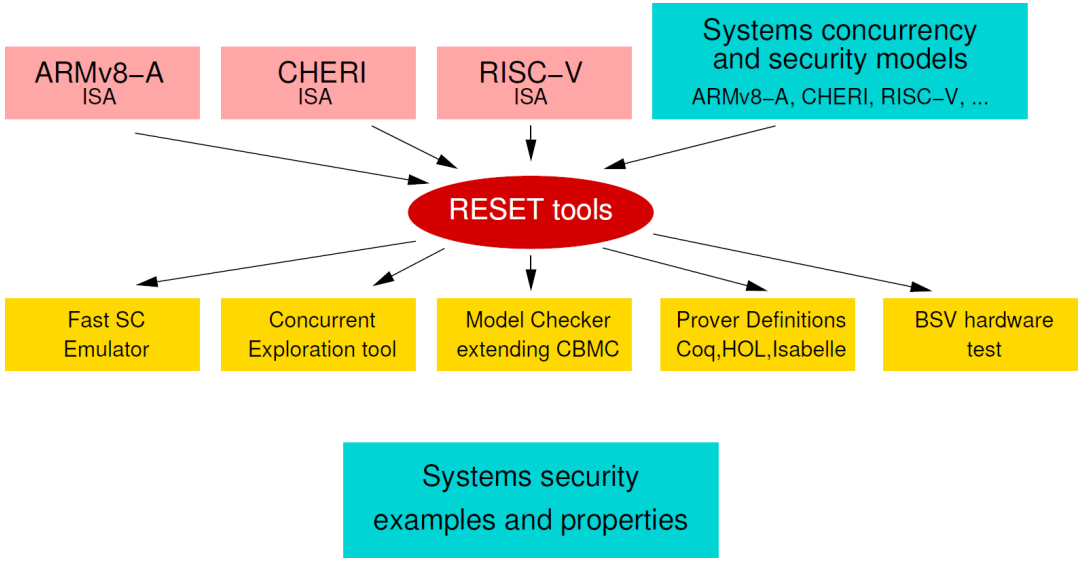
Data intercepted even if phone – server link supposedly encrypted

RESET: Rigorous Engineering for Secure and Trustworthy Systems

System Security : Precise Architectural Models : Modelling, Testing, Proof

SAIL language : CHERI capability architecture ⇒ Microarchitecture : System C : SoC

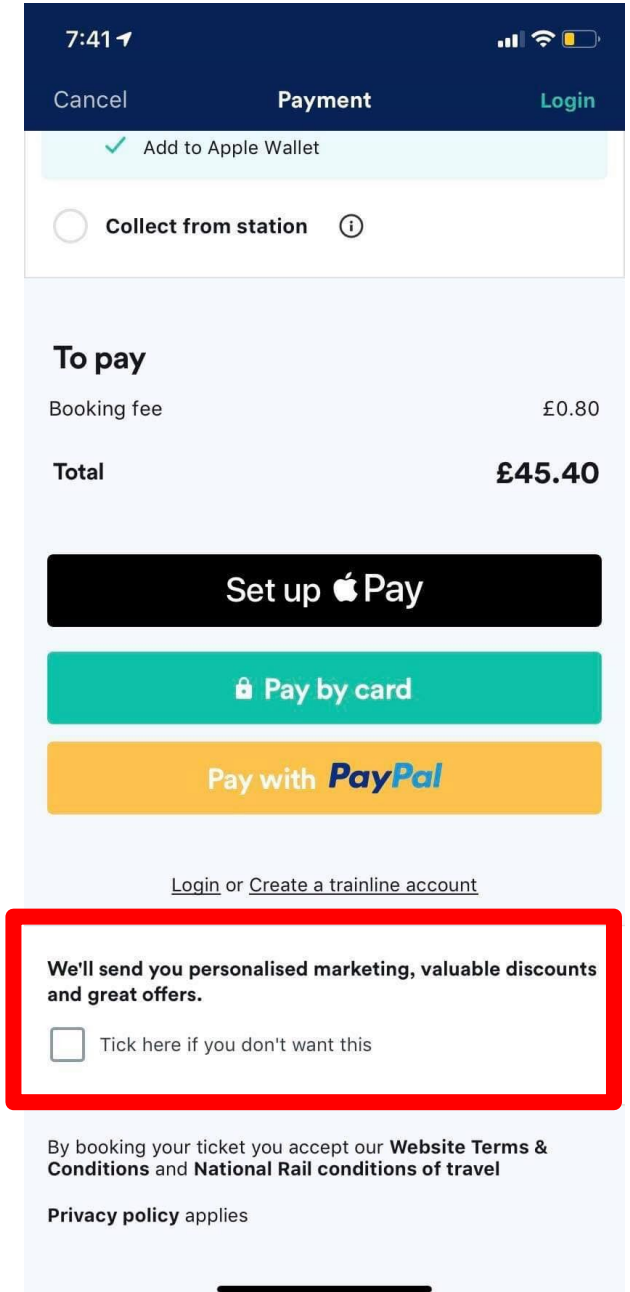




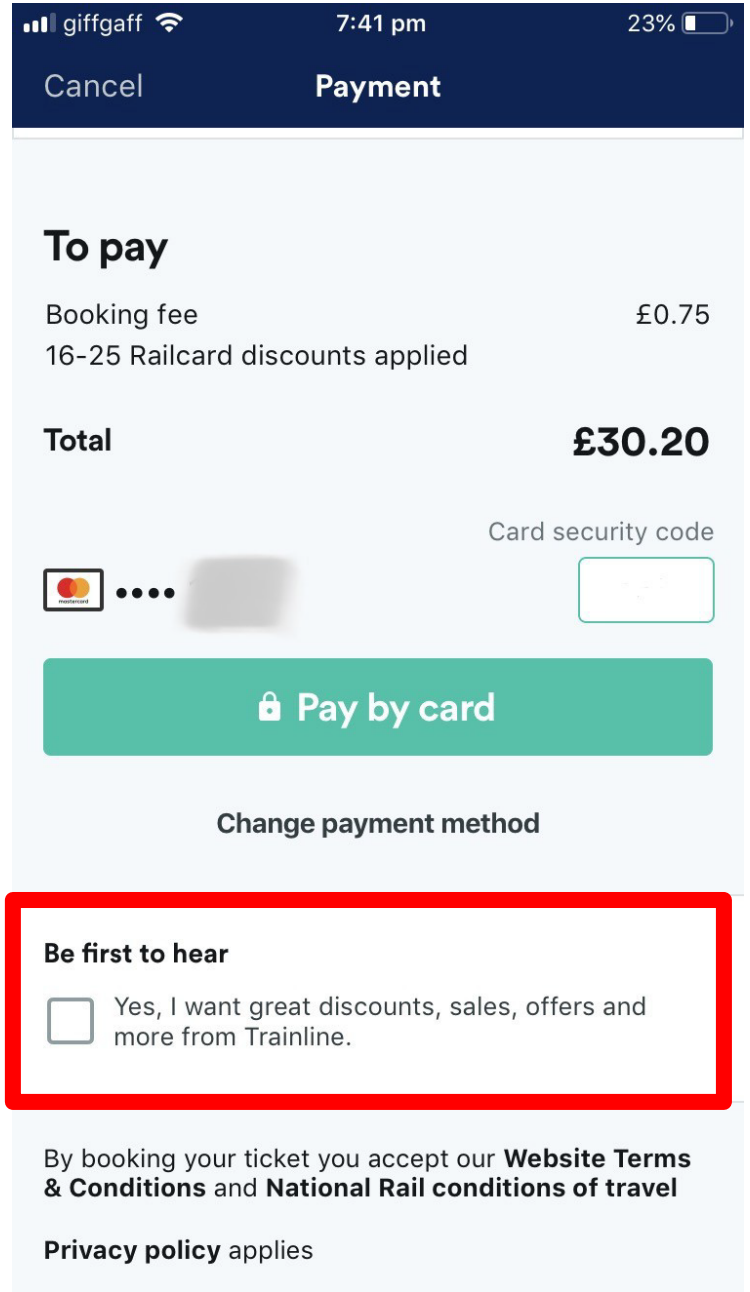
Law and Public Policy

Defining the rules and how they should be interpreted.

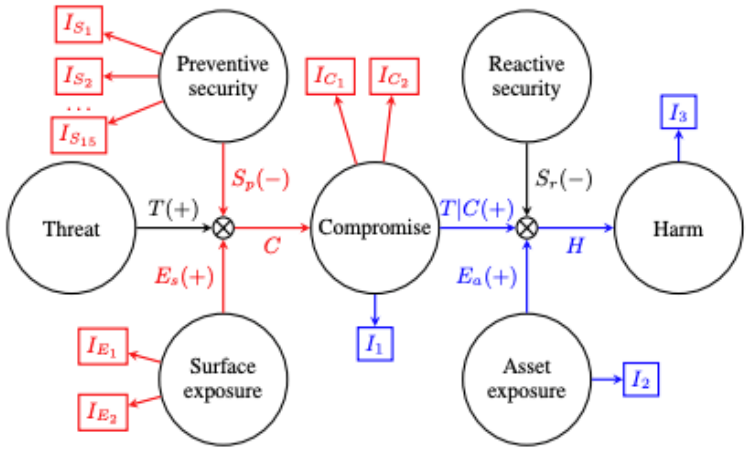
USA Phone



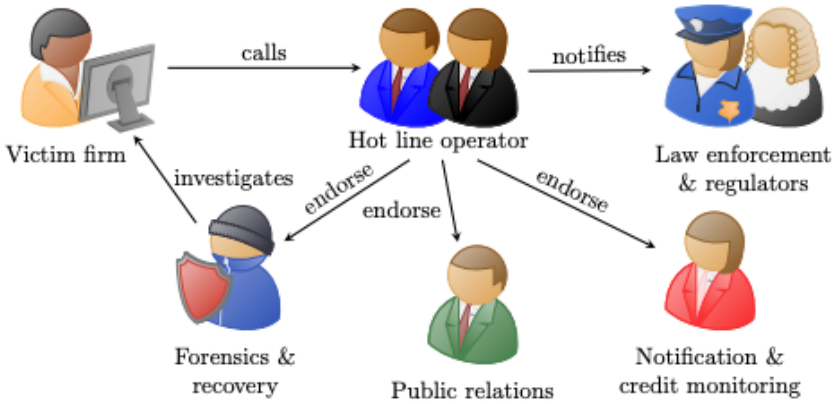
EU Phone



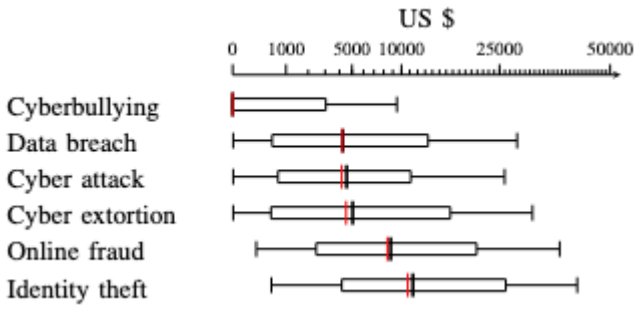
How to measure and manage cyber & privacy risk?



Measuring control efficacy



Crisis management



Measuring harm