Έρευνα & GDPR

Χρήστος Ξενάκης

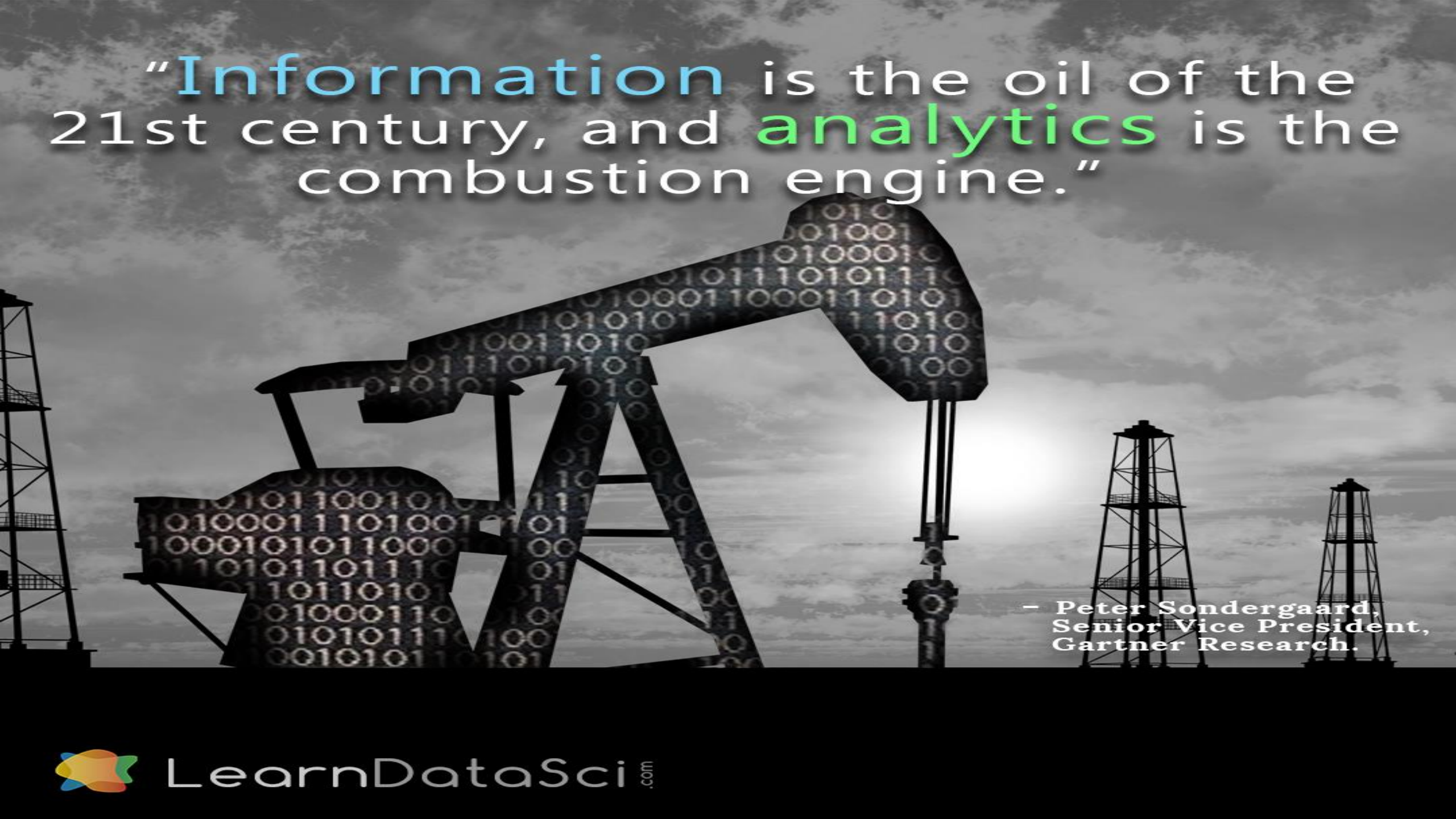
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

UNIVERSITY OF PIRAEUS
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

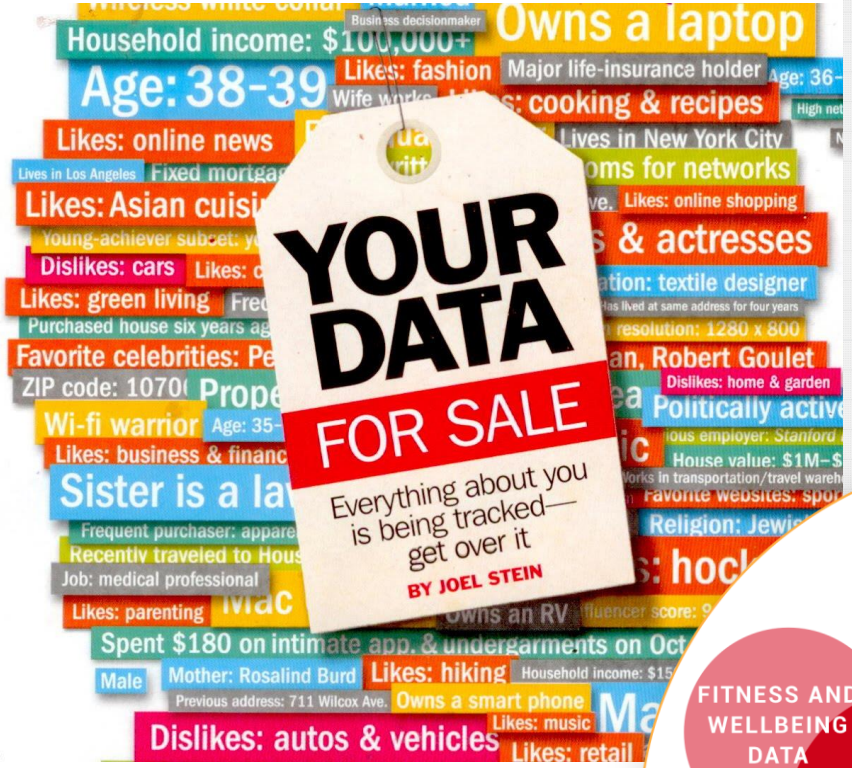
ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

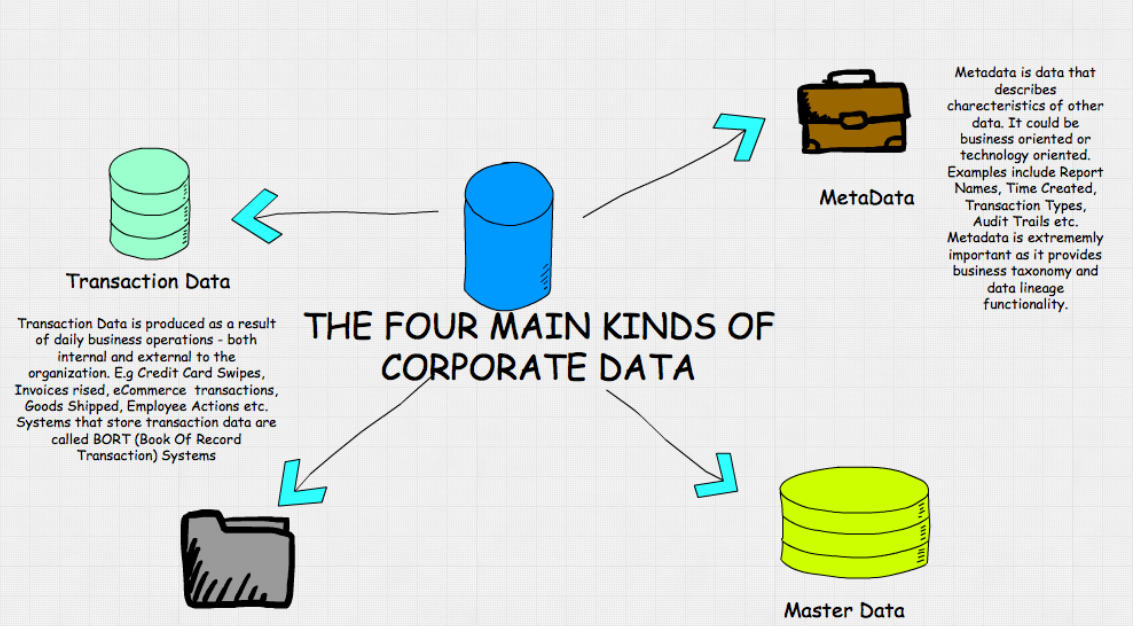
Security Research Lab
University of Piraeus

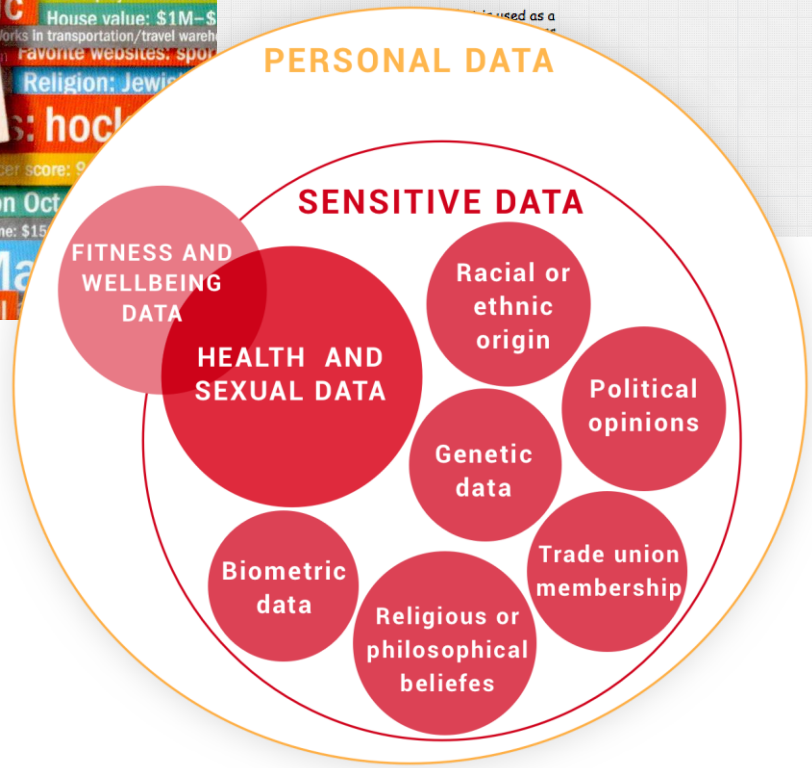
Systems Security
Laboratory


"Information is the oil of the 21st century, and analytics is the combustion engine."
– Peter Sondergaard, Senior Vice President, Gartner Research.
LearnDataSci.com

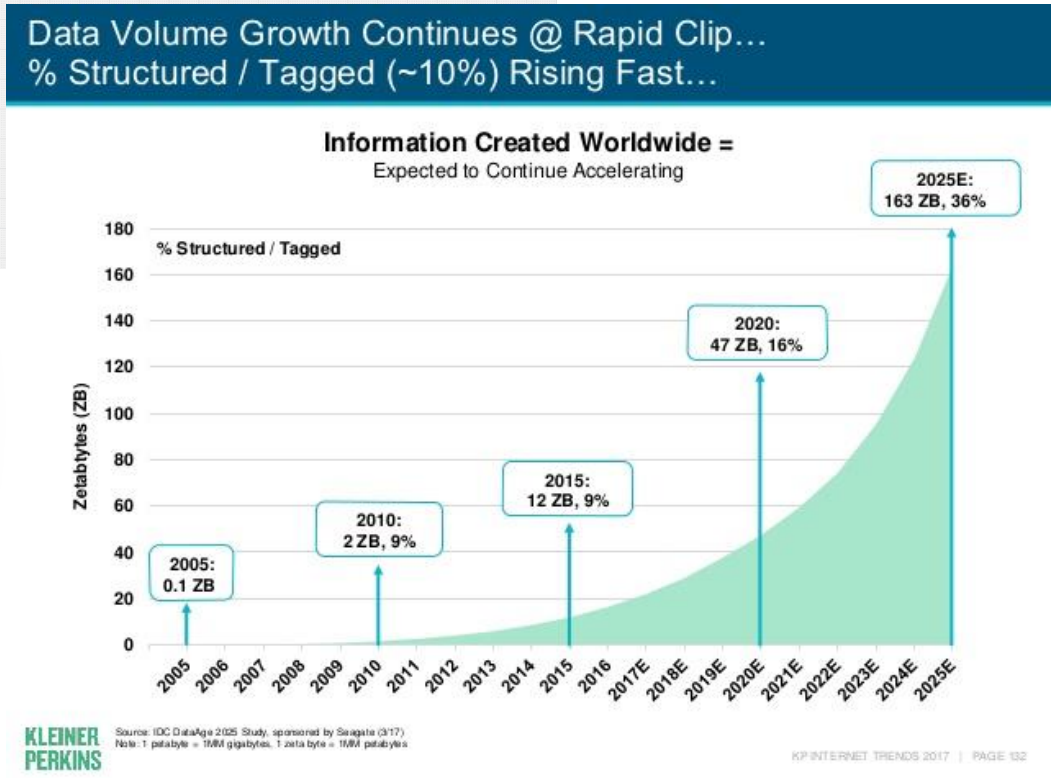
Types of Data

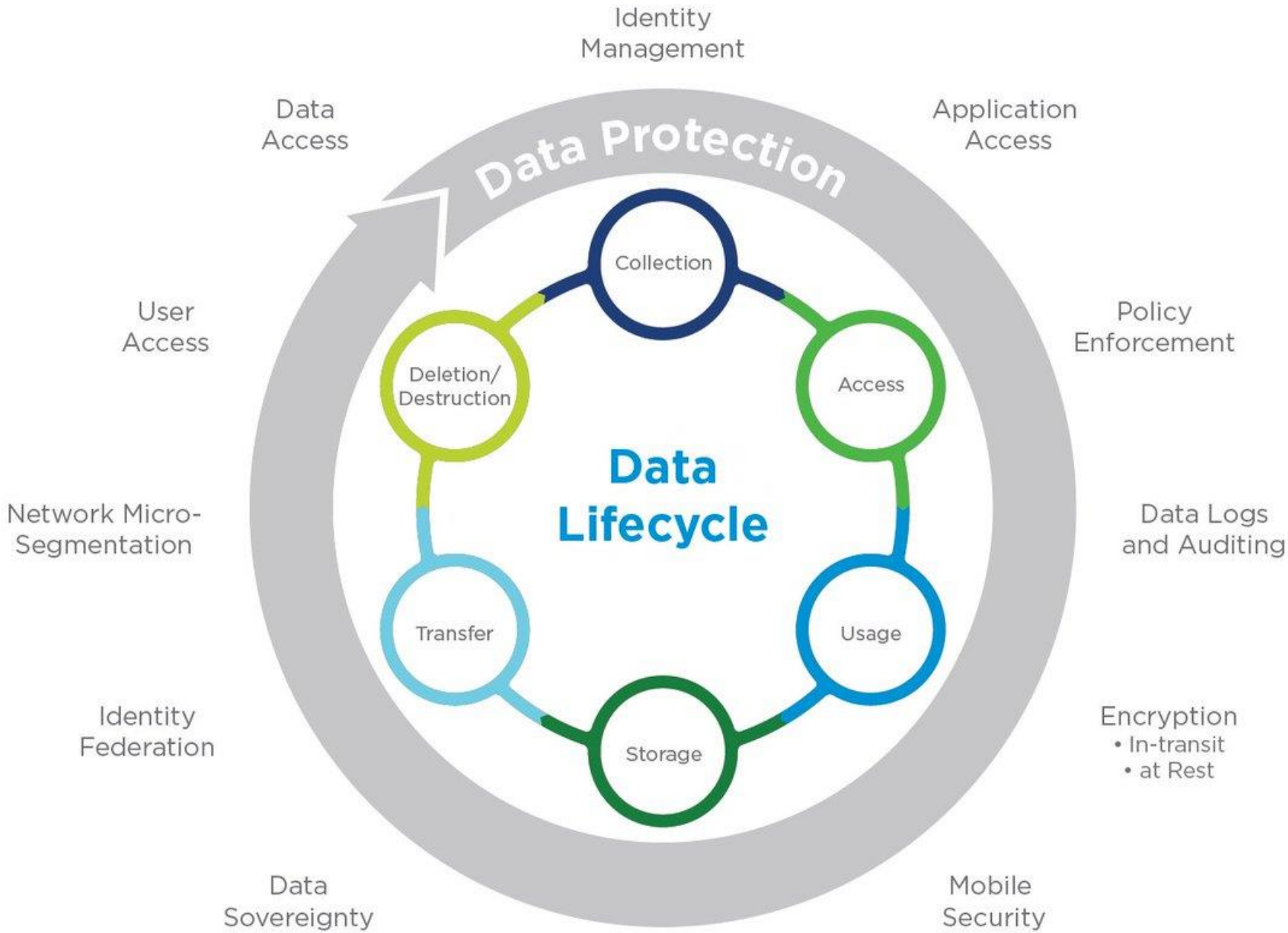


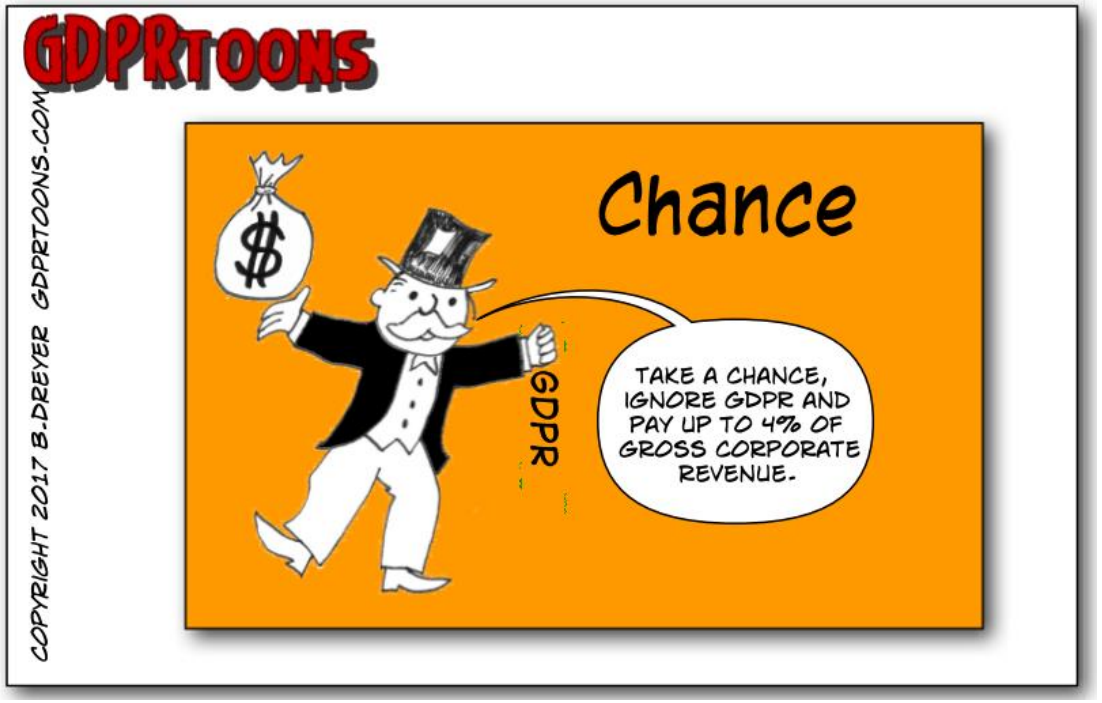




Data Volume Grows exponential




Identity Management
Data Access
Application Access
Data Protection
User Access
Policy Enforcement
Collection
Deletion/ Destruction
Access
Data Lifecycle
Network Micro-Segmentation
Data Logs and Auditing
Transfer
Usage
Identity Federation
Encryption
• In-transit
• at Rest
Storage
Data Sovereignty
Mobile Security

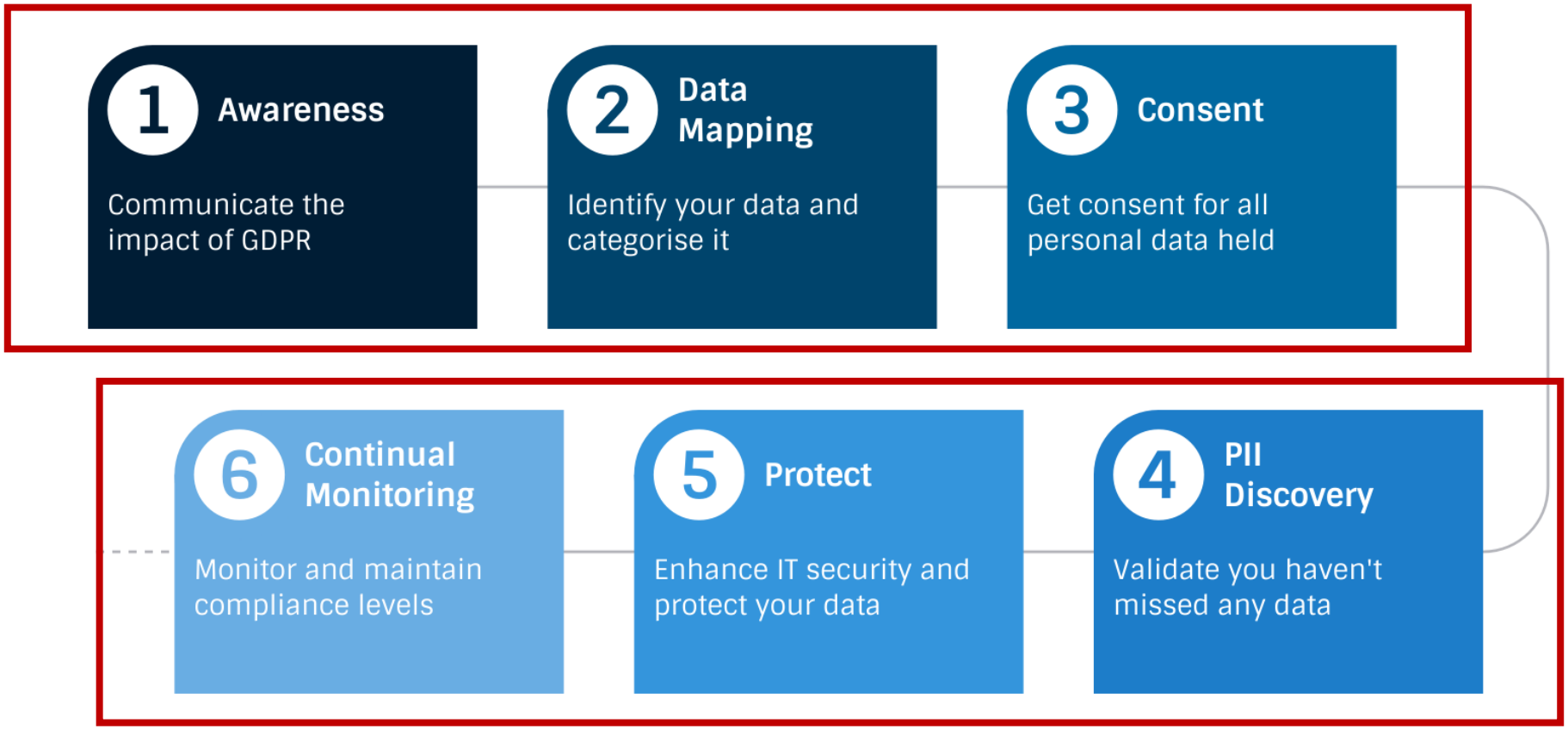


ATTENTION

Cybercrime can no longer be considered as an acceptable 'running cost' of business

Key Steps to GDPR Readiness

Nowadays everybody focuses on these

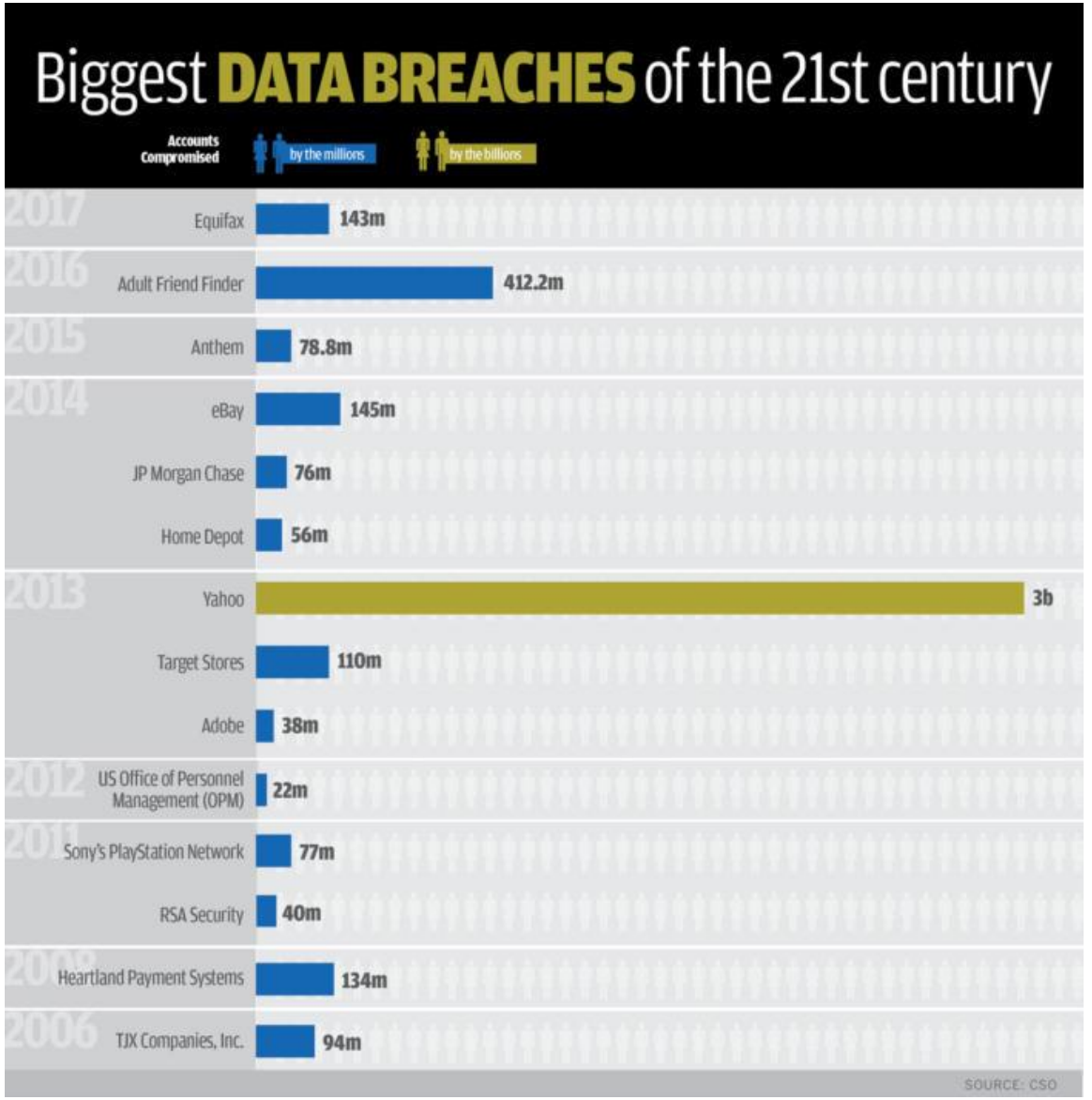


But what about these !!!

Data protection

- Identification
- Identity management
- Access control

The last 8 years more than 7.1 Billion identities have been exposed in data breaches



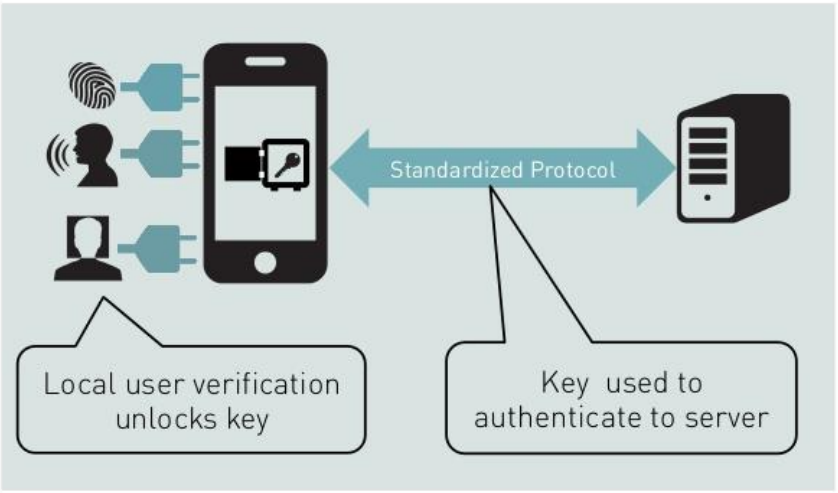
ReCRED

European Commission | Horizon 2020 European Union funding for Research & Innovation

fido alliance simpler stronger authentication

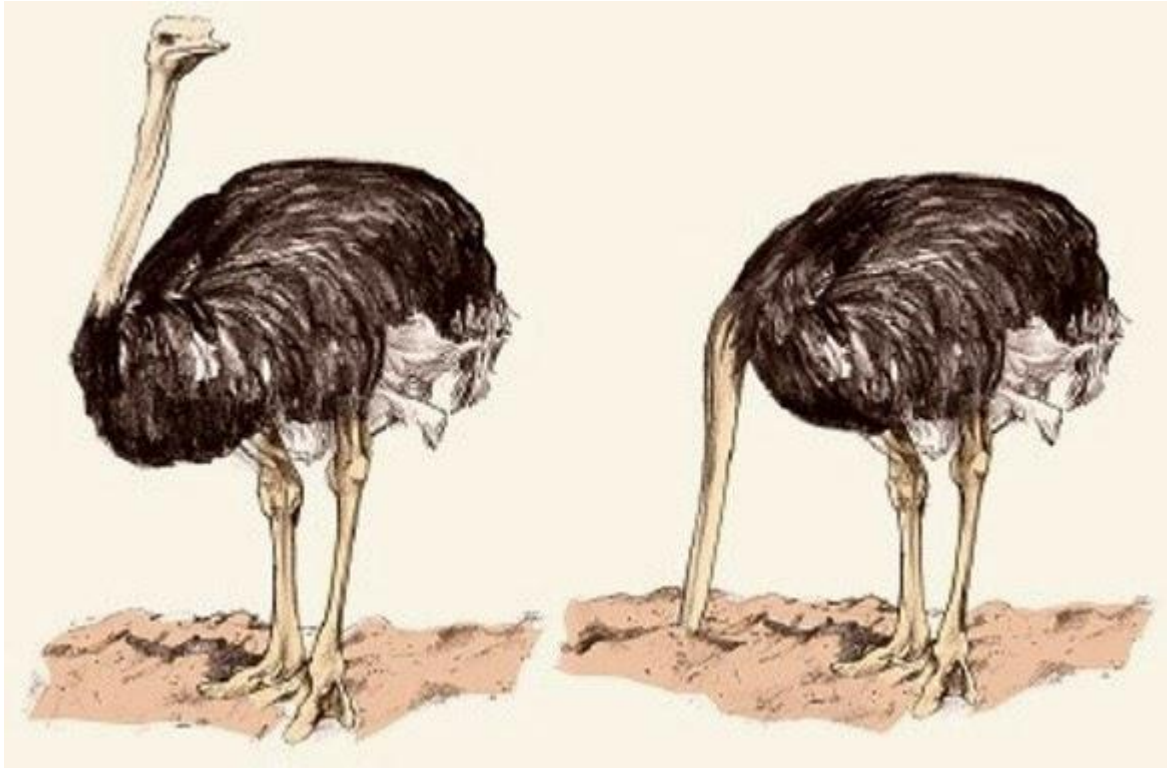
- **Standardized** and **secure** authentication using **FIDO**
  - **FIDO protocol implementation**
- **Multifactor** & **easy to use password-less** authentication
  - Both **biometrics** and **behavioral** authentication
- Renders **password guessing attacks** and **leaks infeasible**

HOW THE FIDO ARCHITECTURE WORKS



Data protection

- Provide anonymity & pseudonymity



- How to distinguish adults from kids
- Provide access control to adults' content

ReCRED

European Commission | Horizon 2020 European Union funding for Research & Innovation

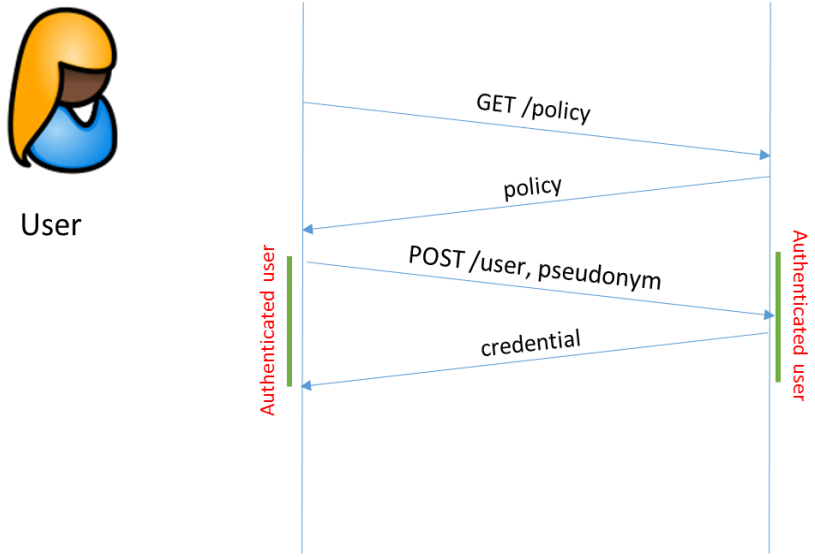
- **Privacy preserving Attribute-based Access Control - Anonymous Credentials**
  - Authentication with **pseudonyms**
- **Account-less access through verified identity attributes**
  - Age, Location, Affiliation, etc.
- **Reveal** to services **only** the **minimum identity information** that is needed
- **Two implementations**
  - **Idemix by IBM**
  - **U-Prove by Microsoft**
- **Advanced cryptography**
  - Zero knowledge, & blind signatures

idemix
pseudonymity for e-transactions

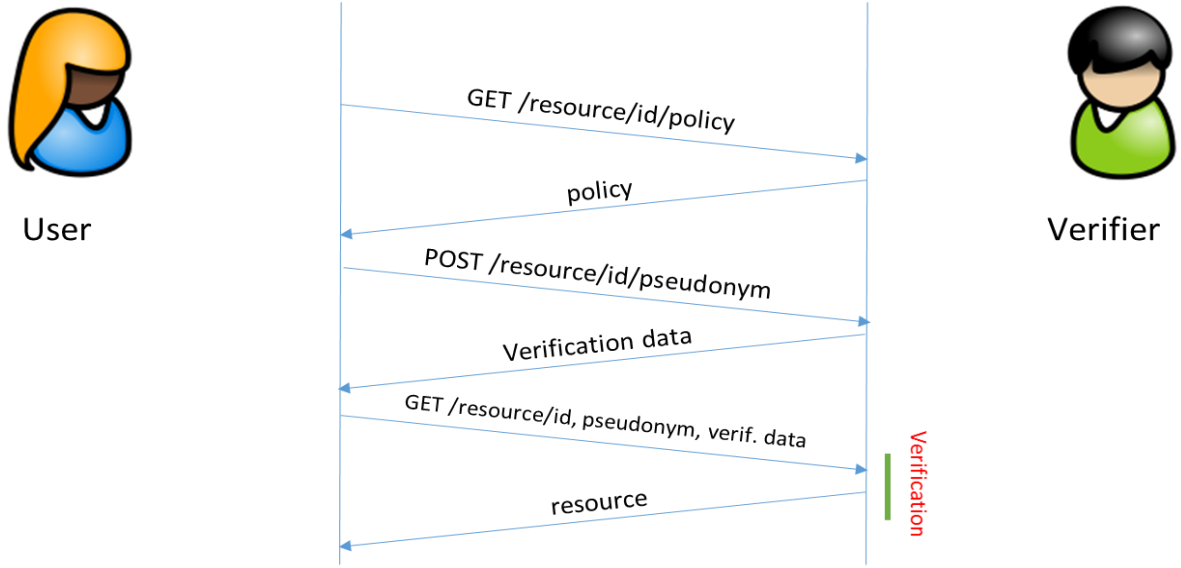
U-Prove

ReCRED

European Commission | Horizon 2020 European Union funding for Research & Innovation



Simplified idemix issuance transaction



Simplified idemix verification transaction

26869985631682372253256636408348855575464066578229061409826643921100627574884, 71763482699009900325890556718198150781635772, 22771015379802672321105 9, 8300470783721158199, 23490470611349108

These attributes have no meaning by themselves

Data protection

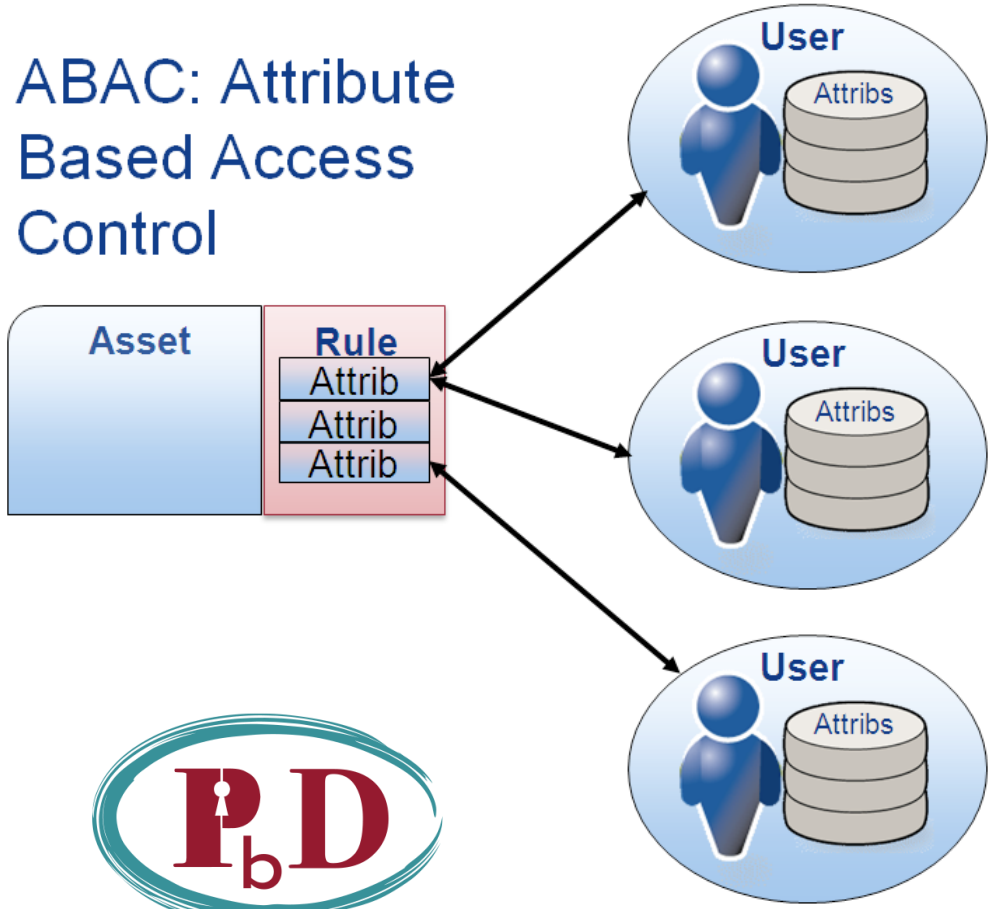
- How can I **control my privacy** & **give my consent** for using my **personal data (GDPR)**
- **Consent management**

JUST SAY "YES"

- It is not a new destination .. It's a new regulation !!!

ReCRED

ABAC: Attribute Based Access Control

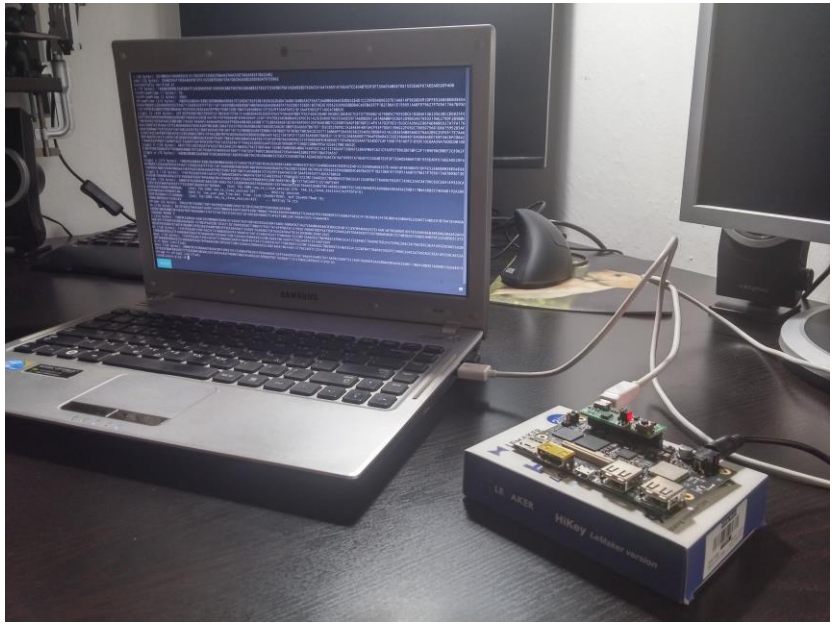


PbD

Privacy by Design

Data protection

- **Security-by-design**
- **Encryption, Confidentiality & Integrity**



ReCRED

- Trusted Execution Environment is a **hardware & software technology** to separate **secure** and **normal** **worlds**
- Provides **hardware root of trust**
- It transfers security from **software** to **hardware**
- **Malware is software** → It cannot **reach** and **tamper hardware**
- **Security functions** are controlled or performed by TEE
  - **Key generation, encryption, decryption, key storage, digital signing, etc**.

Current H2020 R&D projects

- **ReCRED:** From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control (*H2020-DS-02-2014 - Access Control*)
  - **Secure password-less authentication**
  - **Federated identity management**
  - **Privacy-preserving attribute-based access control**
- **UPRC** has the **Project Management**
- Implementation of **FIDO protocol** and **anonymous credentials** inside **Trusted Execution Environment** (TEE)

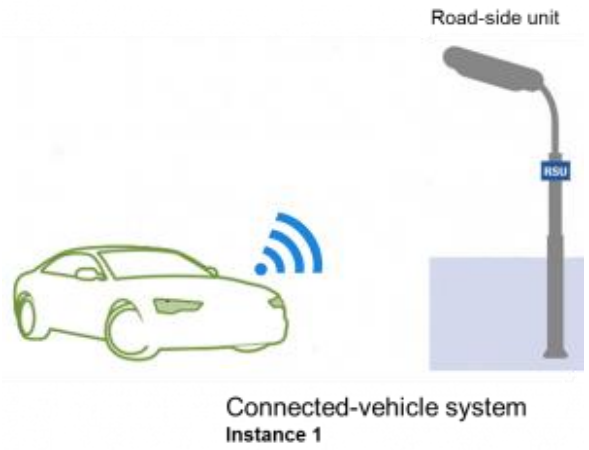
ReCRED

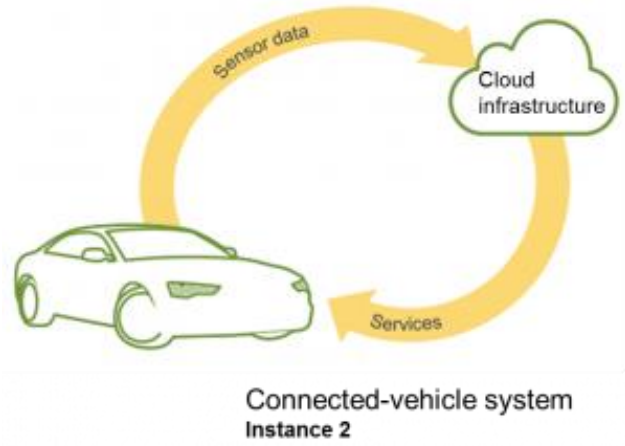
www.recred.eu

Current H2020 R&D projects

- **SAFERtec:** Security Assurance FramEwoRk for neTworked VEhicular TeChnology *(H2020-DS-01-2016)*
  - Modern connected vehicles integrate 3rd party components & applications
  - Numerous interfaces and an increased attack surface is exposed
  - Design and validate a cost-efficient framework for the quantification of security, privacy & safety assurance levels in V2I use-cases
- **UPRC is responsible to design and evaluate the security framework**

https://www.safertec-project.eu/





Current H2020 R&D projects

- **CrowdHEALTH:** Collective wisdom driving public health policies *(H2020-SC1-2016-CNECT)*

- Deliver a **secure ICT platform** to collect and aggregate **high volumes health data** from **multiple information sources** in Europe.

- Proposes the evolution of **patient health records (PHR)** towards **Holistic Health Records (HHRs)** enriched to become **"Social HHRs"** to capture the clinical, social and human factors.

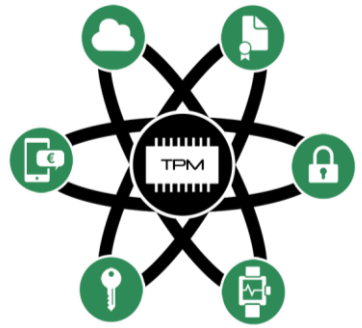
- UPRC is responsible for designing and implementing Single Sign solutions with Attribute Based Access Control (ABAC)

CrowdHEALTH

http://www.crowdhealth.eu/

Current H2020 R&D projects

- **FutureTPM:** Quantum Resistant Trusted Platform *(H2020-DS-06-2017)*
- **Goals**
  - Secure Quantum-Resistant cryptographic algorithms for the TPM
  - Design validation using formal security analysis
  - Implementation for hardware, software, and virtual TPM
  - Real-world applications to tested industrial use-cases
  - Standardization within TCG, ISO/IEC and ETSI
- **Project Results will be validated in three use cases**
  - Online banking
  - Activity tracking
  - Device management



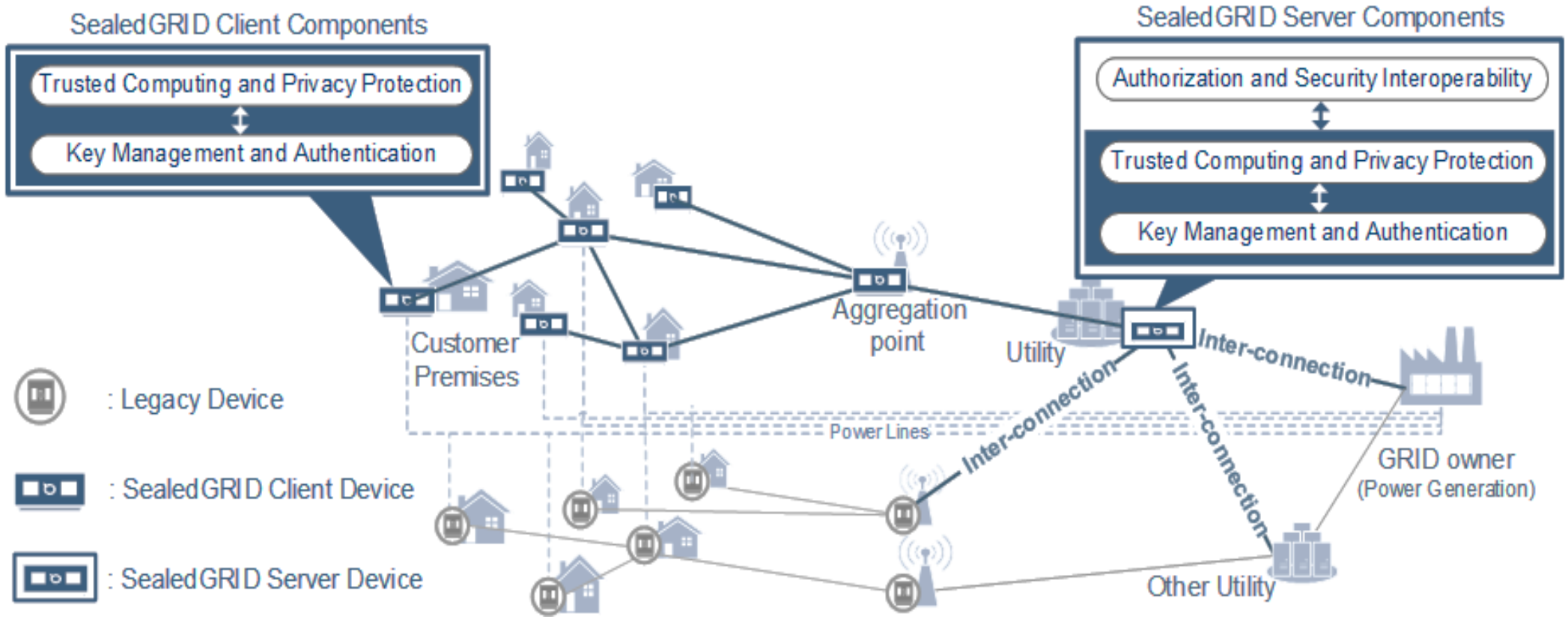
FutureTPM

- **UPRC will contribute to the security analysis and evaluation of the FutureTPM platform**

Current H2020 R&D projects

Network and Information Security

The SealedGRID platform architecture



What else do we need to protect our world ?

The European Cyber Security Challenge - ECSC

- It is an initiative of the **European Commission** supported by **ENISA**
- **Annually**, the competition brings together **young talents** from **European Countries** to have fun and **compete in cyber security**
- The goal of **ECSC** is to place **Cyber Security** at the **service of humankind**
- **Promoting:**
  - **An open, safe and secure cyberspace**
  - **A peaceful society with democratic values**
  - **Free and critical thinking**
- A **Cyber Security championship**

The 2018 European Cyber Security Challenge will be held in London...

2018 Competition Dates

October 15th – 19th 2018

Cyber Security Challenge UK

The Greek Participation

- The **leadership** for the **Greek participation** in **ECSC 2018** was appointed to the **Systems' Security Laboratory** of the **Department of Digital Systems** of the **University of Piraeus**
  - Constitution of the **Greek Team**
  - Organization of the **Greek participation**
  - Financial administration – Sponsorship
  - Dissemination
- The **Steering Committee** members are:
  - Prof. Christos Xenakis
  - Prof. Costas Lambrinoudakis

HELLENIC CYBER SECURITY TEAM

University of Piraeus
Department of Digital Systems

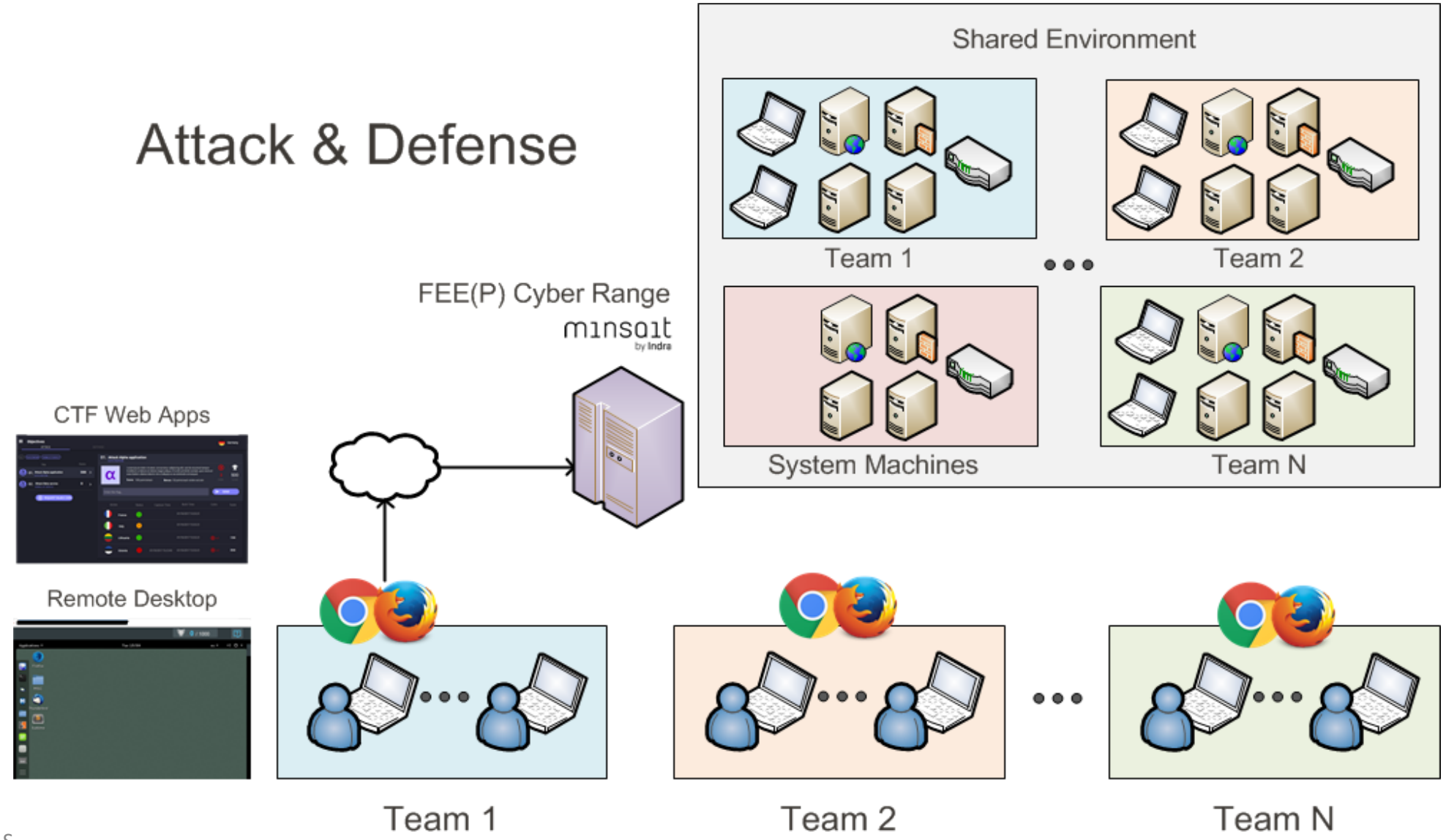
The Hellenic Cybersecurity Team

- **10 Persons - Contestants**
  - Should be selected by a **National Competition**
  - **Five person (14-20)** and **five person (21 – 25)** who legally reside in **Greece**
- Three **coaches** (an additional may act as alternative) who is responsible for
  - **Well-being** and **behavior** of the **Greek Team**
  - Making sure that **essential information** reaches the **Team** and is **understood**
  - **Organizing the Team's strategy**
- **A Jury representative**
  - One from each country that assess the **performance**

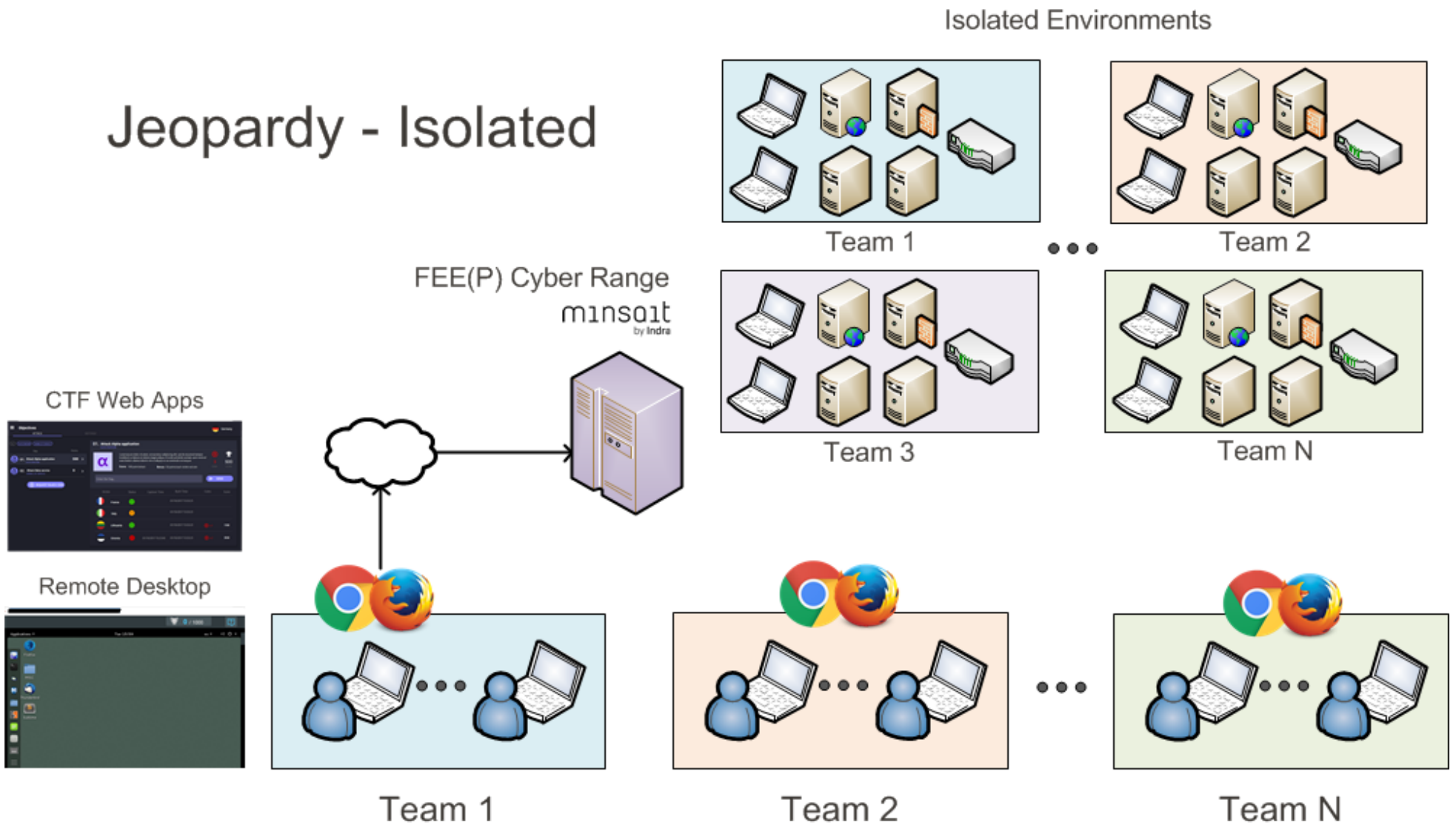
Competition

- It will be based on the **educational exercise Capture-The-Flag (CTF),** which gives the participants experience in:
  - **Securing** a **machine** or an **application**
  - **Conducting** and **reacting** to **attacks** found in the **real world**
- Challenges will include:
  - **Reverse engineering, network sniffing, protocol analysis**
  - **System administration, programming, cryptoanalysis**
  - **Web security, forensics, mobile security**
- In both styles: (a) **attack/defense** and (b) **Jeopardy**

Competition - CTF



Competition - Isolated



Competition - Required skills


Operating Systems


Forensic Analysis


Web Hacking


Crypto Puzzles


Malware Analysis


Reverse Engineering


Social Engineering


Mobile Security


Esteganography


Database Security


Code Analysis


Cryptography


Secure Programming


Penetration Testing


Network Security


Miscellaneous

Objectives for the Hellenic Team in 2018

- Attract more than **> 100 participant** at the **National Competition**
- Constitute a team of more than **> 20 persons** of the two age sets **(14- 20) & (21 – 25)**
- **Create a Hellenic Cyber Security Academy**
  - Contestants, Coaches, Supporters, Professionals, Researcher, etc.
- **Attract more Sponsors**
- **Higher impact** and **exposure** to **the media / society**
- Become more **self-funded** by providing:
  - **Professional services**
  - **Cyber training**

www.ecsc.gr

@ECSC2017HellenicTeam

European Cyber Security Challenge - Hellenic Team

@ECSCGR

xenakis@unipi.gr stet@ssl-unipi.gr ecsc@unipi.gr