Research Activities in the Area of Privacy

Christos Xenakis

Systems Security Laboratory (http://ssl.ds.unipi.gr/)
Department of Digital Systems, University of Piraeus

UNIVERSITY OF PIRAEUS RESEARCH CENTER

UNIVERSITY OF PIRAEUS

University of

A few words about us …

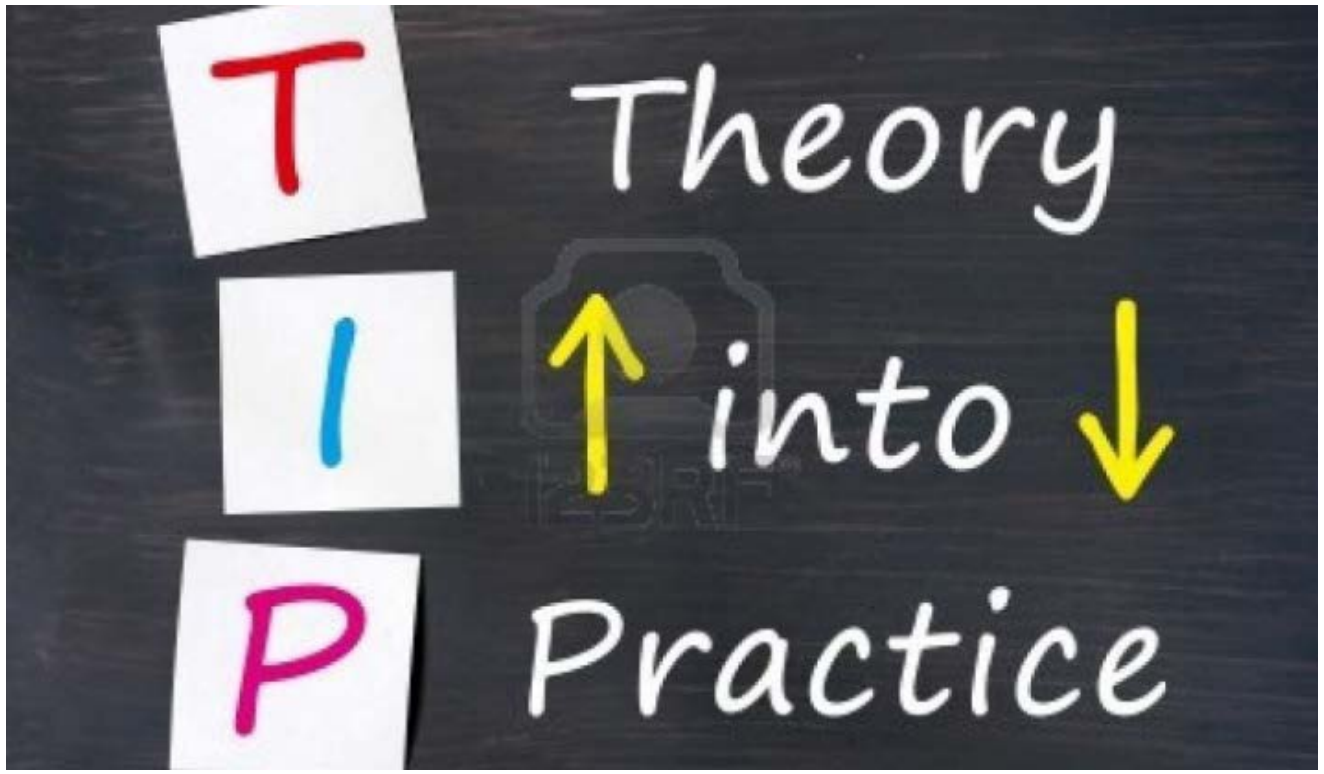
- University of Piraeus, Greece
- School of Information and Communication Technologies
- Department of Digital Systems
- System Security Laboratory founded in 2008
- Research, Development & Education
  - systems security, network security
  - computer security, forensics
  - risk analysis & management
- MSc course on "Digital Systems Security" since 2009

Before R&D !


Hope
test
holidays
technology
LEADERSHIP
SCHOOL
GUIDANCE
STUDY
ASSIGNMENT
INTELLIGENCE
FOCUS
EXPERIENCE
COLLEGE
LECTURER
dorm
YOUNG
pressure
IDENTITY
HOBBY
challenge
LEARN
tuition
LOANS
SKILLS
AWARDS
commitment
dedication
scholarship
FRIENDSHIP
SUCCESS
Job
FUN
EDUCATION
FUTURE
INDEPENDENCE
SOCIAL
hardwork
achievement
UNIVERSITY
DREAMS
YOUTH
GOALS
SPORTS
CREDIBILITY
OPPORTUNITIES
FREEDOM
relationship
occupation
FUTURE
GRADUATION
WORK
class
INNOCENCE
smart
Laboratory
extracurricular
COMPETITION
teacher
Ambition
hardWORK
EMPLOYMENT
books
mentor
RESEARCH
Students

What we do for education

- **Undergraduate studies ….**
  - Security Policies and Security Management
  - Information Systems Security
  - Network Security
  - Cryptography
  - Mobile, wireless network security
  - Privacy enhancing technologies
  - Bachelor Thesis

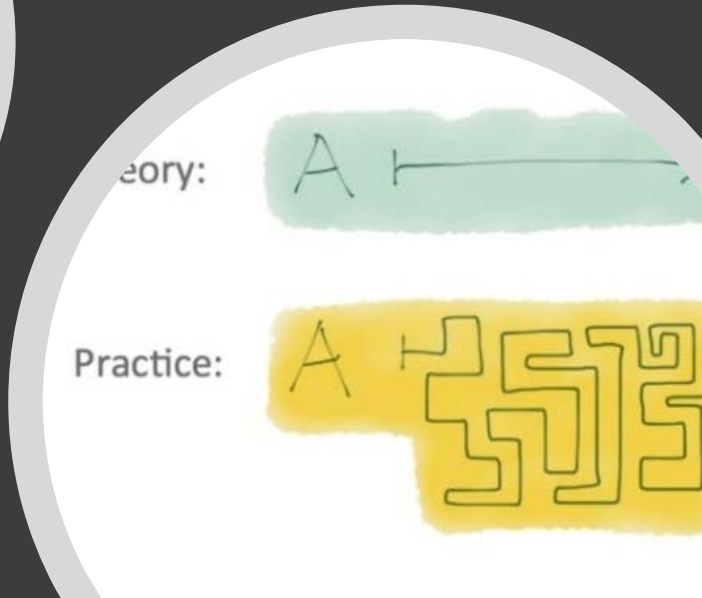


Post-Graduate Lessons

- **Postgraduate studies in Digital Systems Security**
- **1st semester**
  - Applied Cryptography
  - Information Systems Security and Privacy Protection
  - Network Security
  - Security Assessment and Vulnerability Exploitation

Post-Graduate Lessons

- **Postgraduate studies in Digital Systems Security**
- **2nd semester**
  - Research Methodology
  - Mobile Internet Security
  - Digital Forensics and Web Security
  - Legal Aspects of Security



Post-Graduate Lessons

- Postgraduate studies in Digital Systems Security
- 3rd semester
  - Master Thesis

  - ISO 27001
  - Certified Information Security Manager (CISM)
  - DPO certification

System Security Laboratory

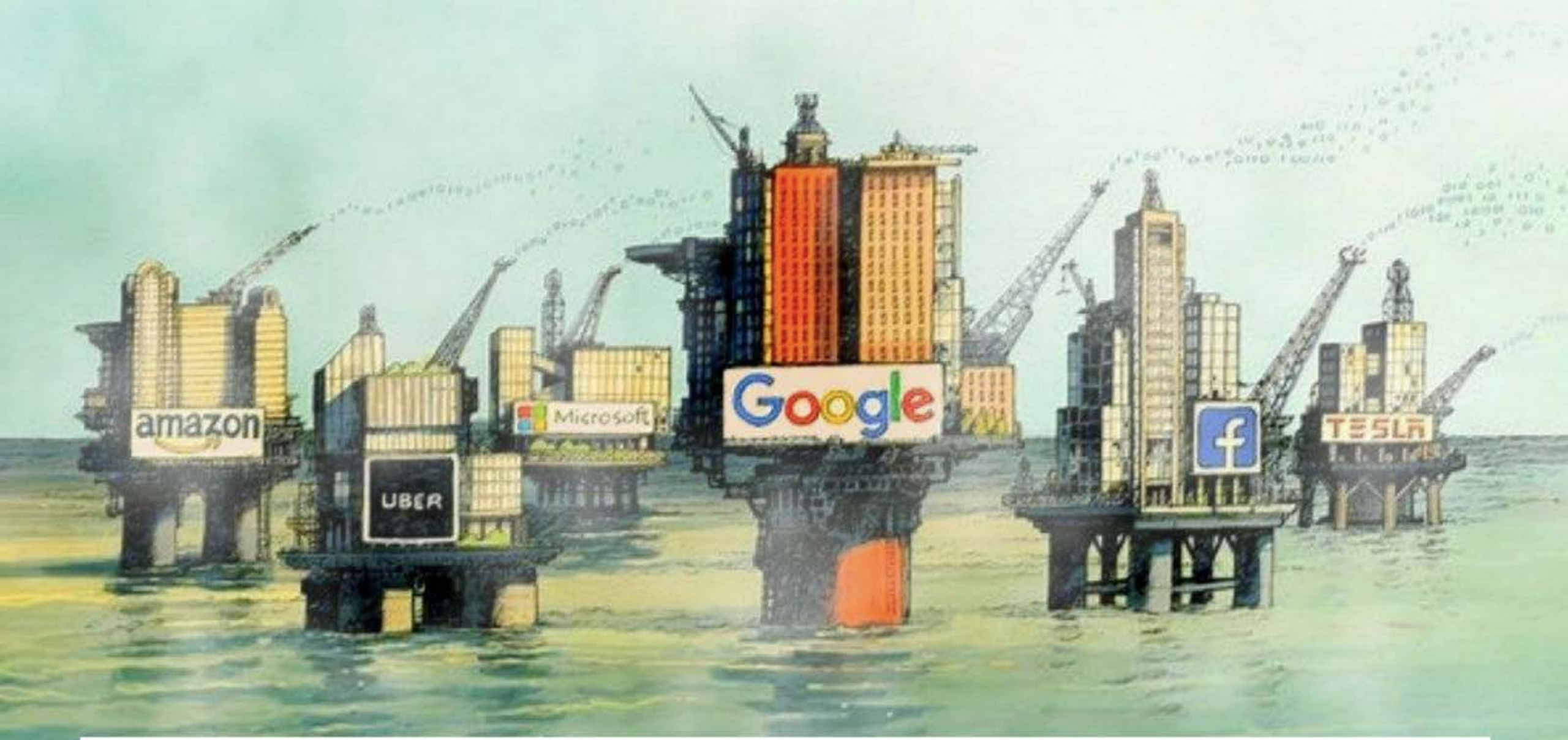
- **Costas Labrinoudakis**, *Professor, Head of the Department, Director of the Lab*
- **Christos Xenakis**, *Associate Professor, Director of the Master Course*
- **Christoforos Ntantogian**, *Research Associate, Chief of the Lab*
- **Stefanos Malliaros**, *Research Assistant*
- **Eleni Veroni**, *Research Assistant*
- **Christos Lyvas**, *Research Assistant*
- **Farnaz Mohammadi**, *Research Assistant*
- **Anna Aggelogianni**, *Research Assistant*
- **Aris Farao**, *Research Assistant*
- ***Panagiotis Bountakas***, *Research Assistant*
- ***Vaios Bolgouras***, *Research Assistant*
- ***Nikolaos Koutroubouxos,*** *Research Assistant*

Areas of Expertise

- **Smart Grid and IoT security**
  - Authentication, key management, trust management, privacy solutions, lightweight intrusion detection
- **Mobile – Wireless networks**
  - Security evaluation, security solutions, quantitative risk analysis

- **Network security**
  - Identity management, password-less authentication, access control, trust management, anonymous authentication, remote attestation
- **Computer Security**
  - Trusted computing, AV evasion using ROP techniques

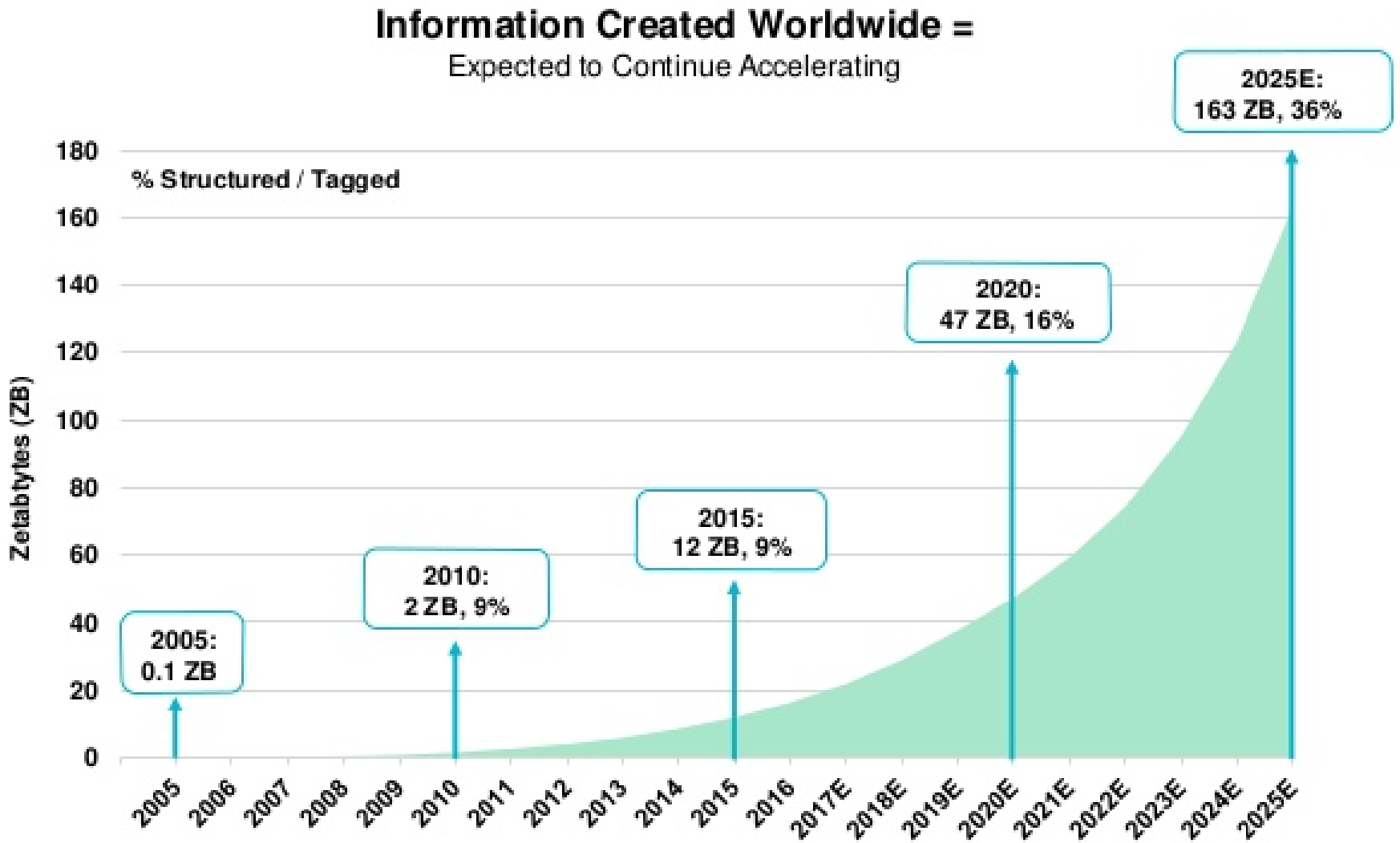
- **Security evaluations & penetration testing**
  - Web, mobile systems, embedded systems, mobile – wireless networks, core telecom networks, SCADA



The world's most valuable resource is no longer oil, but data.

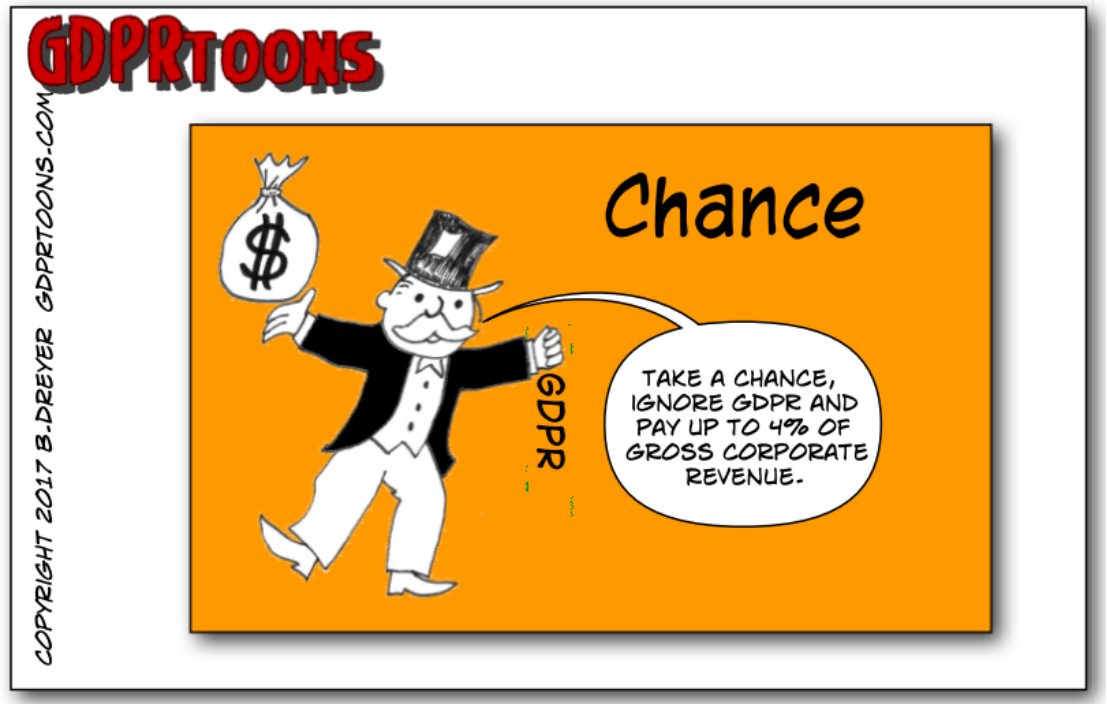
The Economist - May 2017

Data Volume Growth Continues @ Rapid Clip…
% Structured / Tagged (~10%) Rising Fast…



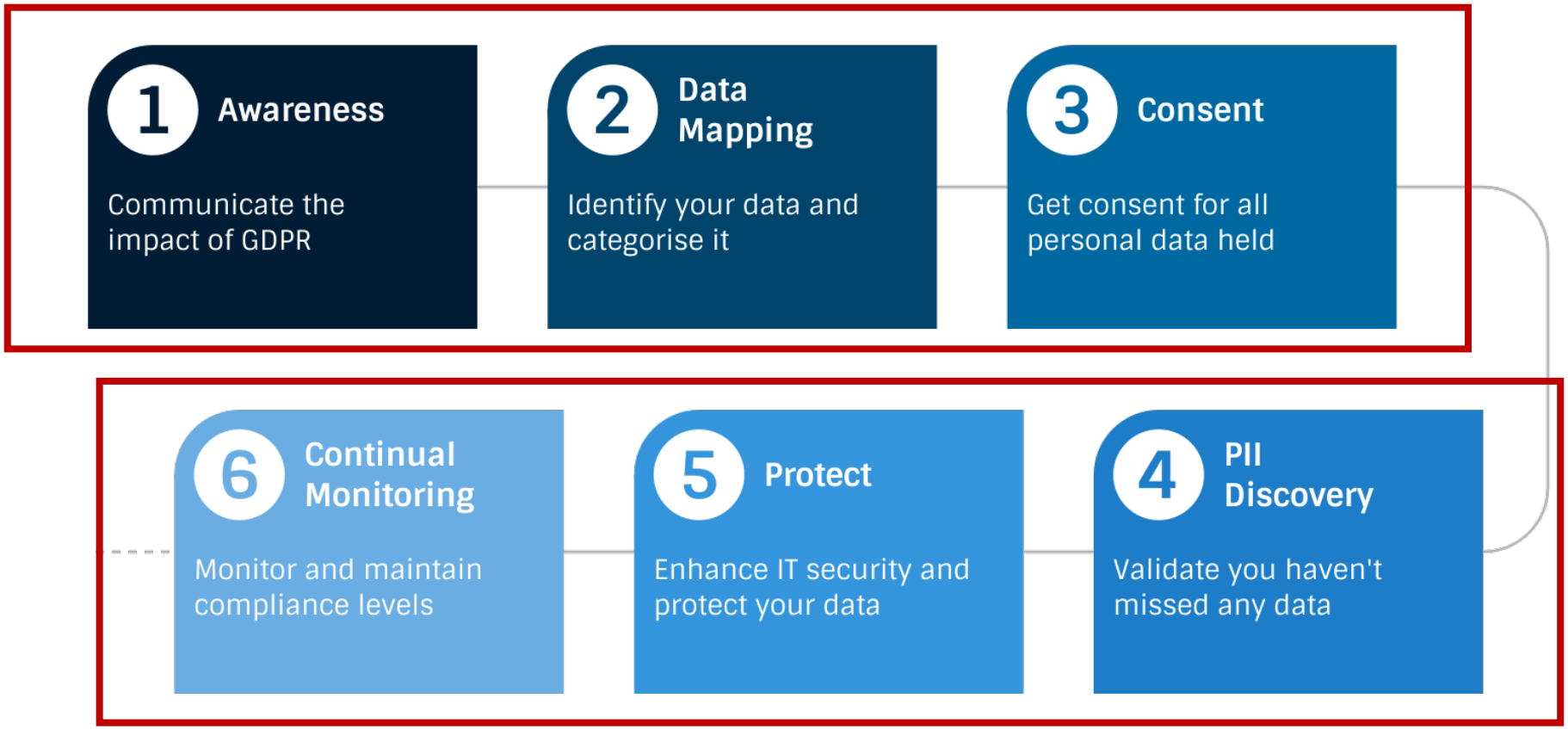
Source: IDC DataAge 2025 Study, sponsored by Seagate (3/17)
Note: 1 petabyte = 1MM gigabytes, 1 zetabyte = 1MM petabytes

General Data Protection Regulation – GDPR



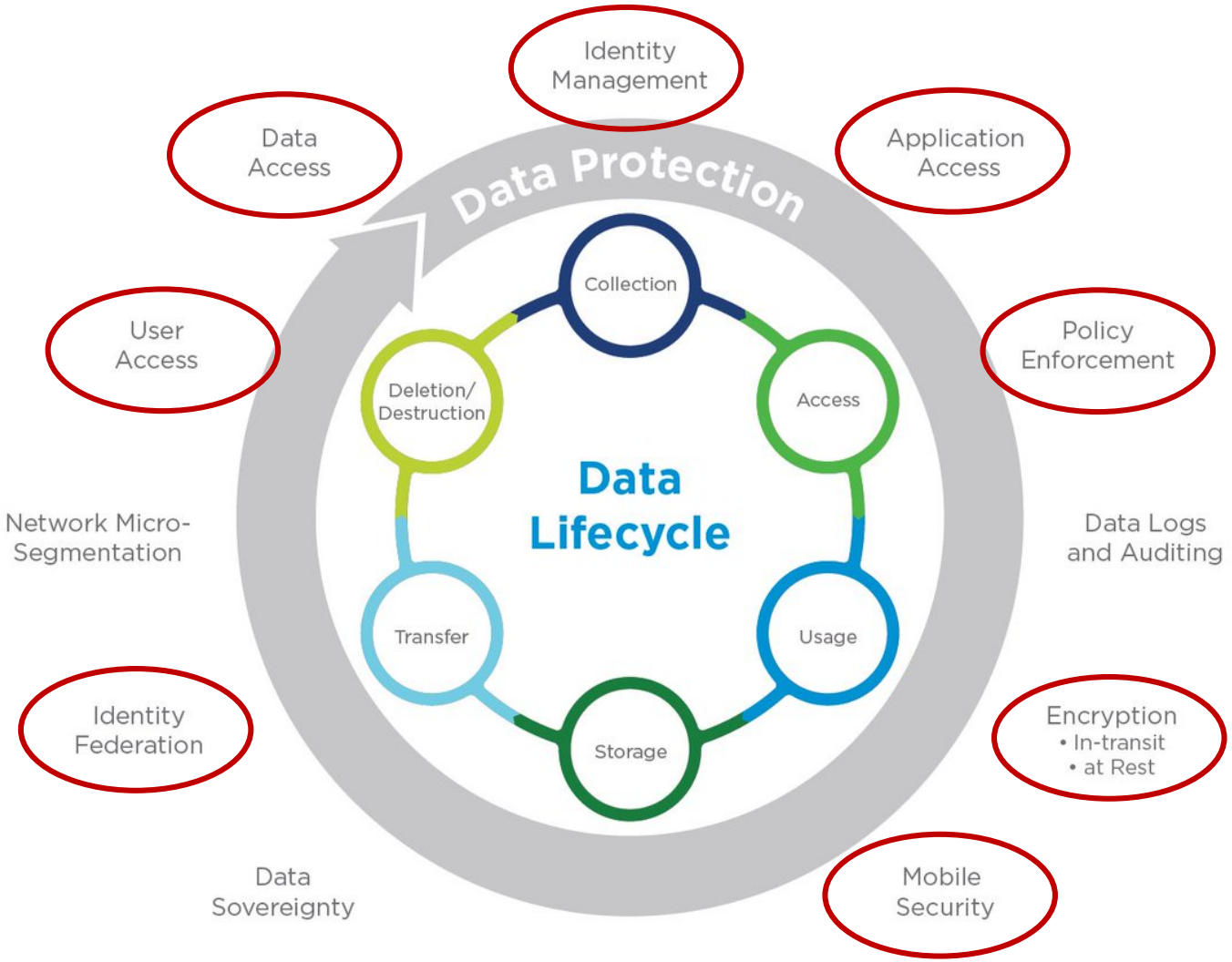
Key steps to GDPR readiness

Nowadays everybody focuses on these



But what about these !!!

Data Lifecycle, Data Protection and ReCRED solutions



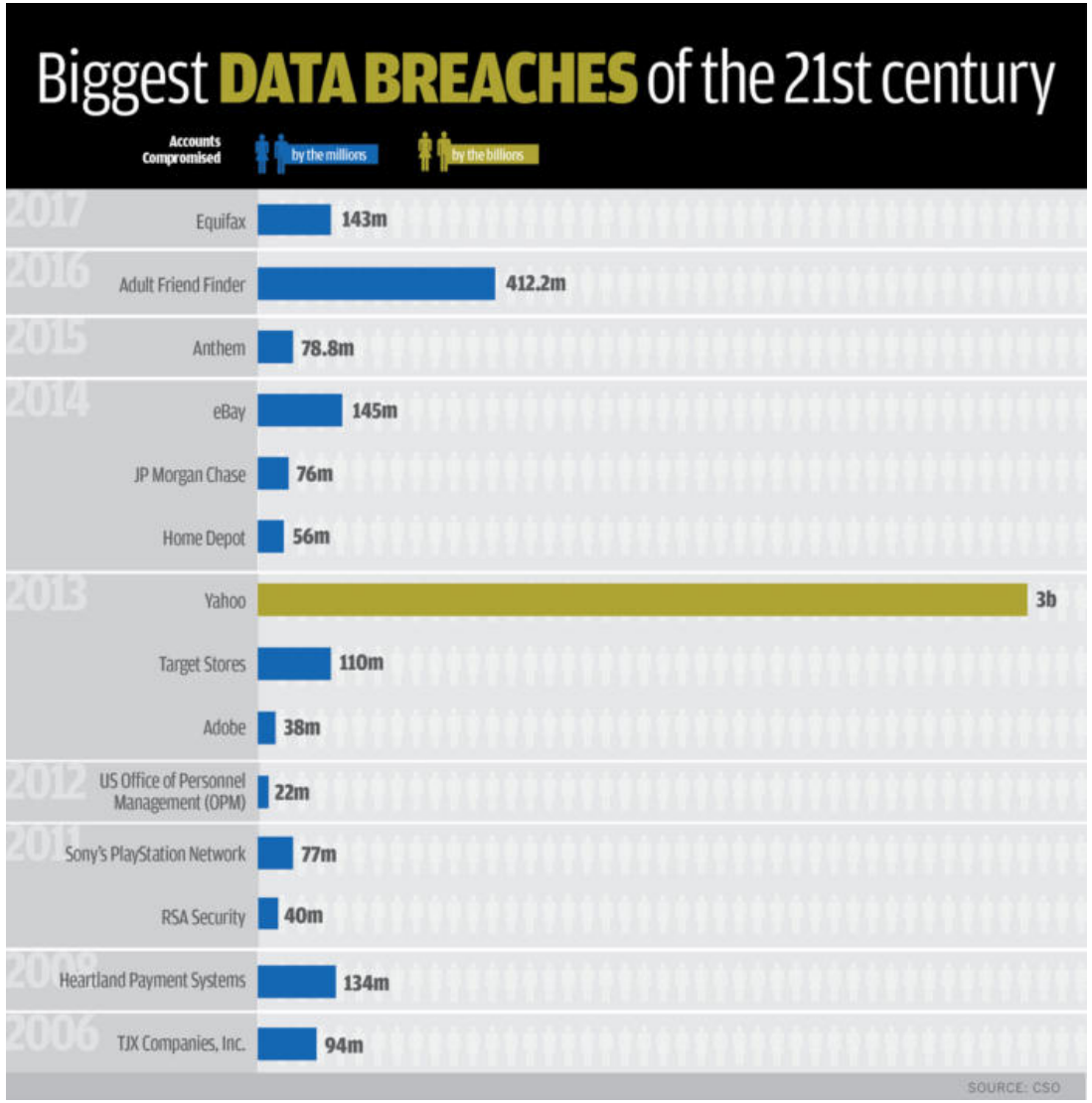
- **ReCRED's solutions focus on**
  - **Identity Management**
  - **Application Access**
  - **Policy Enforcement**
  - **Encryption**
  - **Mobile Security**
  - **Identity Federation**
  - **User Access**
  - **Data Access**

Problem 1: What happens with Passwords ?

- **Users authentication** is the basis for **Data Protection** and specifically for:
  - **Identity Management**, **Application Access**, **User Access** & **Data Access**
- Currently, **user authentication** relies **on passwords**
  - a **technology of the '60s**
  - **98%** of the **websites** use **password-based authentication**
  - **70%** of users **forget their password once in a month**

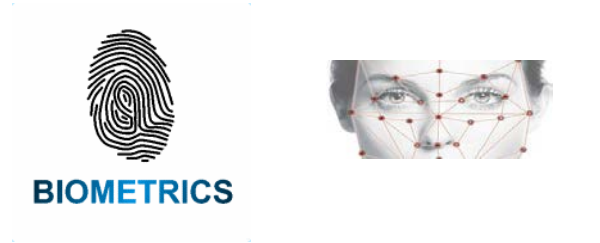
Problem 1: What's wrong with Passwords ?

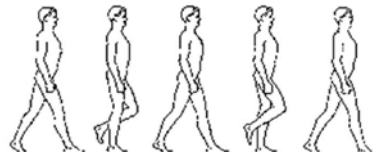
- Users have the **tendency** to choose **weak** & **easy-to-remember** **passwords**
- Passwords are **highly** **reused** **by users**
- Many **cyber attacks** are initiated by **compromising credentials** or **exploiting weak passwords**.
- Nearly, **one** out of **every two cyber attacks** saw **breach of password**
- The last 8 years more than **7.1 Billion identities** have been exposed in **data breaches**



ReCRED's solutions to the problem of passwords

- **Standardized** and **secure** authentication using **FIDO**
  - **FIDO protocol implementation** that provides **Device Centric authentication**
- **Multifactor** & **easy to use password-less** authentication
  - **Biometrics** and **behavioral** authentication for 1st & 2nd factor authentication
- It offers **strong authentication** based on **public key cryptography**
- It **enhances users' privacy** since all **identifying info** is stored **locally**
- Renders **password guessing attacks** and **leaks infeasible**





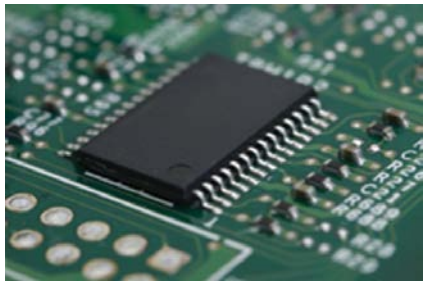
What is the provided level of protection ?

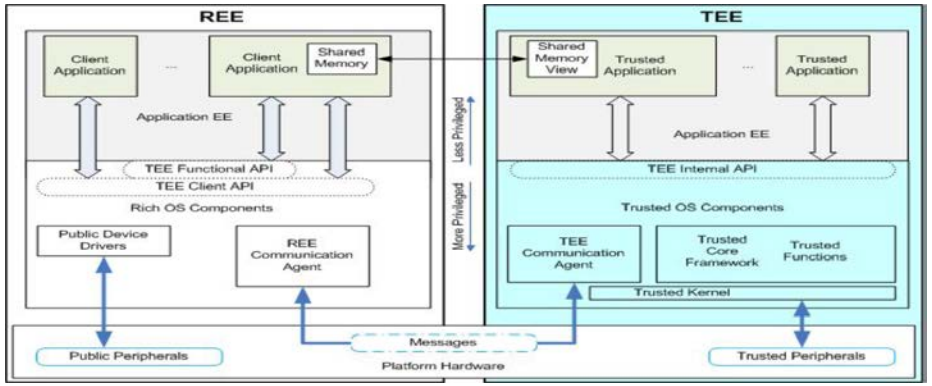
- My mobile device is the **gateway** to my **digital life**
- What If my mobile device is:
  - **Compromised** 
  - **Stolen** 
  - **Broken** 
  - **Lost** 
  - **Replaced** 

ReCRED supports Security-by-Design

Security-by-Design - I: Trusted Computing

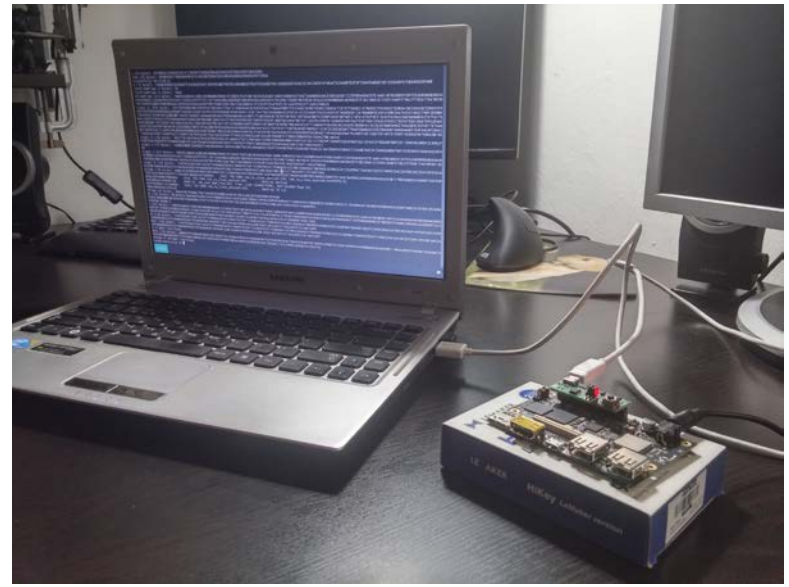
- **Trusted Execution Environment**
  - It is a **hardware & software technology** to separate **secure** and **normal** **worlds**
  - Provides **hardware root of trust**
  - It transfers security from **software** to **hardware**
  - **Malware is software** → It cannot **reach** and **tamper hardware**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





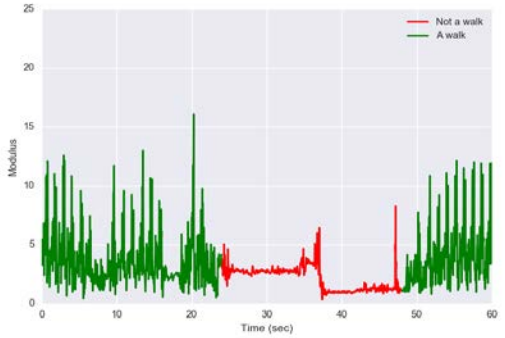
Security-by-Design - I: Trusted Execution Environment - TEE

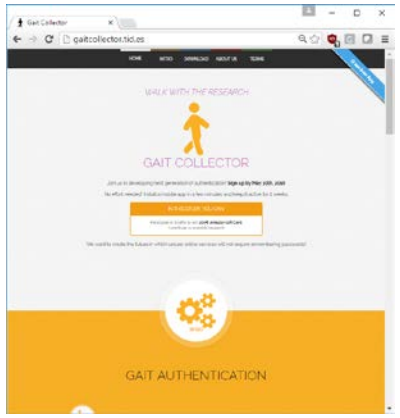
- Within **ReCRED** we are using three **different TEE**:
  - **ARM TrustZone** included in many **off-the-self mobile devices**
  - **Open-TEE** emulation environment
  - **OP-TEE** real operating system
    - We are using a **HiKey** board and a **Rpi 3**
    - Both incorporate **ARM TrustZone** technology
    - We used **an open source TEE for Linux** named **OP-TEE**
    - Hardware debugging (**JTAG** & serial)

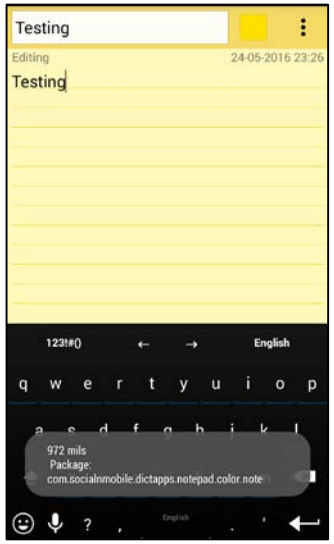


Security-by-Design - II: 2nd or 3rd factor Authentications

- Within **ReCRED**, we have developed **four** different types of **behavioral authentications**:
  - Key stroke
  - Browsing habits
  - Mobility
  - Gait
- Latch for account locking







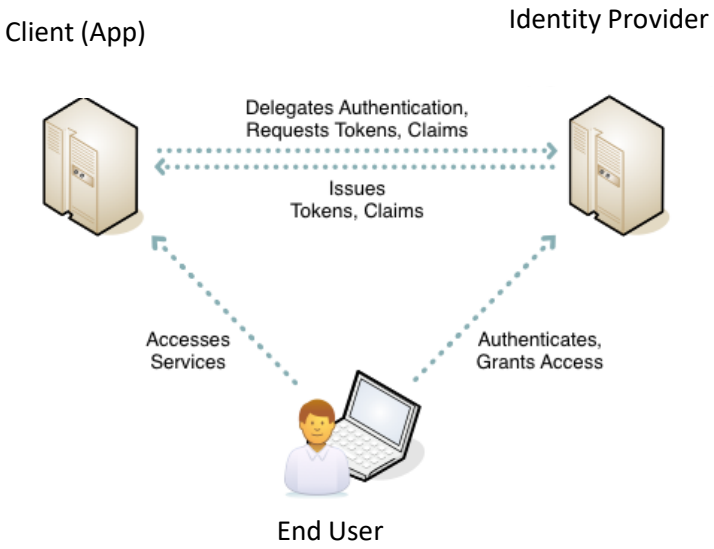
Problem 2: Identity Fragmentation – Online Accounts

- Today's Internet users are registered in **too many online services**
  - Gmail, Yahoo, Facebook, Twitter, LinkedIn, e-banking, dropbox, etc.
  - Each one use a **different authentication method** & **credentials**

- **Questions arise:**
  - Can I **consolidate** & **manage securely** all these **identities & accounts**
  - Can I **link** my **online accounts** e.g., facebook with google
  - Can I **link** an **online account** with my **physical identity** e.g., e-bay to sell my laptop **(3rd problem)**

FIDO – Federated authentication - OpenID Connect

- **OpenID Connect** (federated authentication) delegates authentication
  - Online services authenticate their users by employing **Google**, **Microsoft**, **Twitter**, **LinkedIn** accounts, etc.
- **OAuth 2.0** (Open standard for Authorization)
  - Issues and uses **access tokens** to be used for **authorization**
- **User: less passwords** to remember
- **Service providers:** no need for **password maintenance**
- **ReCRED's approach** = **Fido+(OpenID Connect/OAuth2.0)+BAA**



Problem 2: Identity Management – Consent Management

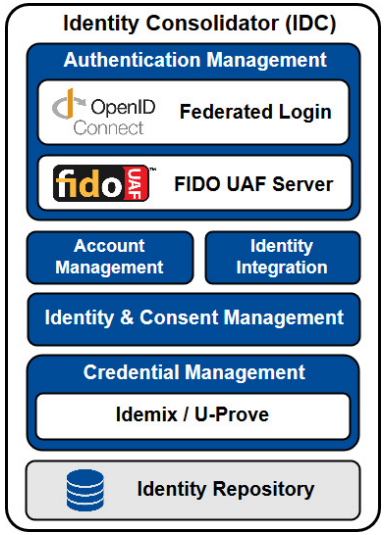
- How can I **control my privacy** & **give my consent** for using my **personal data**
- Currently I simply **reply to an email** or just say: **YES**

JUST SAY "YES"

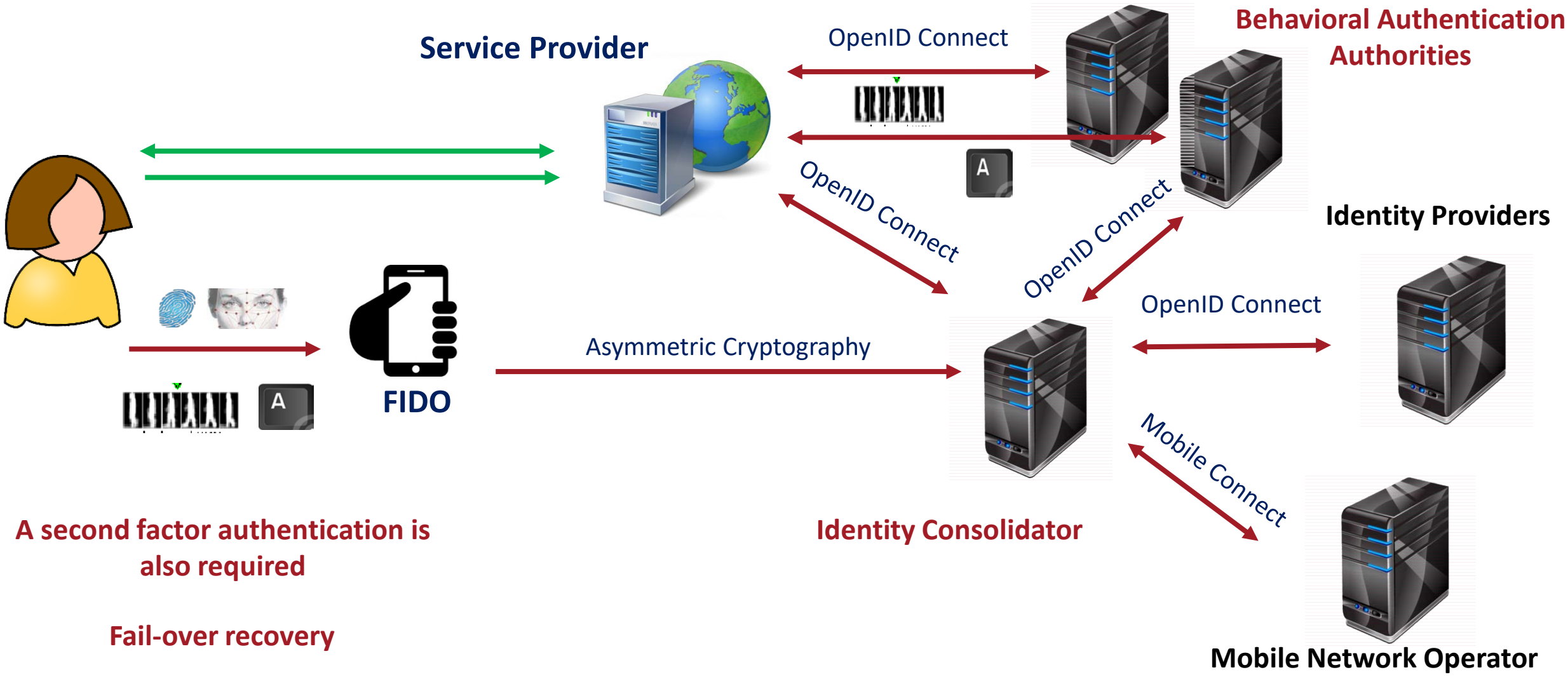
- It is not a new destination .. It's a new regulation !!!

ReCRED's solutions: Identity consolidation & management

- **Identity Consolidator** is the central entity of **ReCRED**
  - It is a **identity provider (idp)** , that acts a **trust third party** and provides **users' authentication**
  - Manages all **access control needs** of the users and supports **federated authentication**
    - Using my **UNIPI account**, **gmail account**, **BAA**, **Vodafon subscription**, etc.
  - It **issues** and **verifies** **cryptographic credentials** *(we will talk about this later on…)*
  - Performs **fail-over recovery** (in case of lost or damaged devices)
  - It may horizontally **bind** the **online identities** of a users
  - Collects **identity attributes** from various IdPs **upon user's request**
  - Enables users to **control the level of privacy** on their **personal data**
  - For data usage, **users' consent** **is required**



Device Centric Authentication - DCA

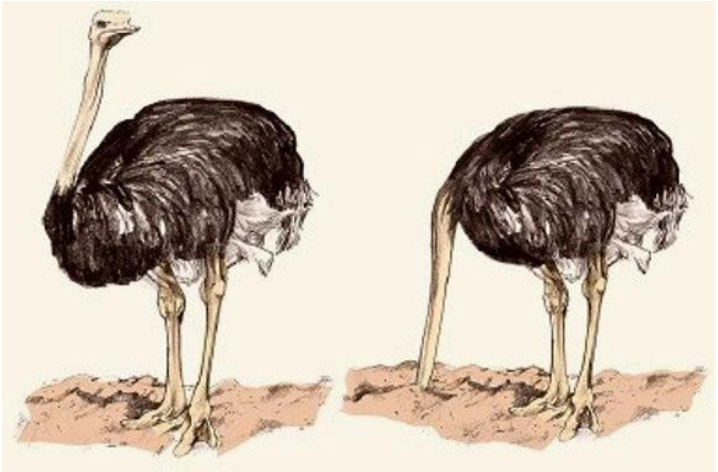


Problem 4 : I want Anonymity

- **But, OpenID Connect** does not provide any **anonymity !!**
- I want to have access to an online bookstore **that has a discount if I have the specific attributes** or **properties:**
  - I am **over 22**
  - I am a **student**
  - I am **EU citizen**
- I want to **ensure my anonymity controlling my privacy**
  - **I do not want to reveal any additional personal information**

Problem 4 : Privacy-by-Default

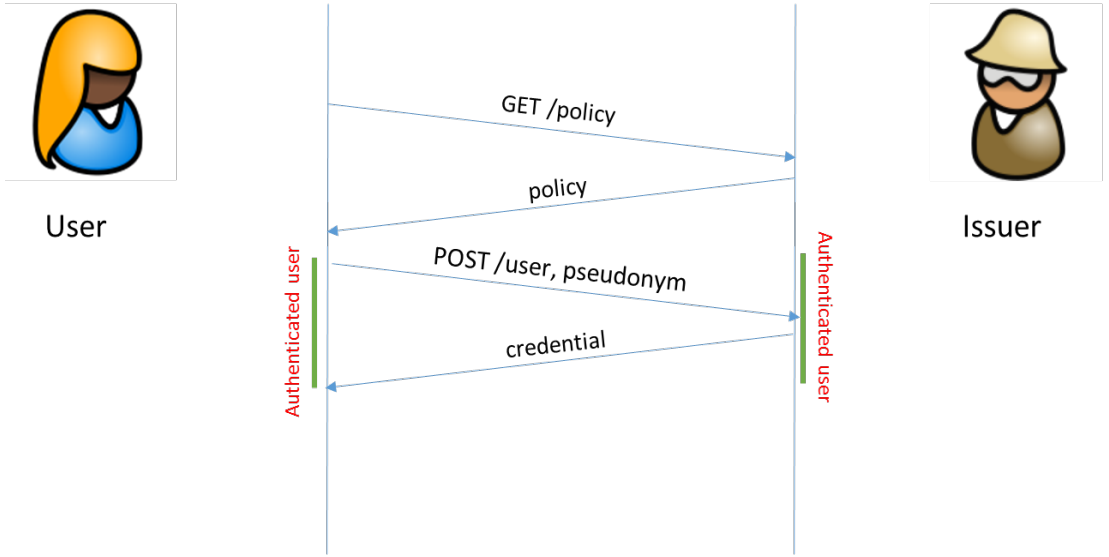
- Some real **life's problems** that require **controlled privacy**
  - How to provide **anonymity** & **pseudonymity** to **online servi**ces
  - How to distinguish **adults** from **kids online**, while **preserving anonymity**
  - How to provide **access control** to adults' content, **ensuring anonymity**
- **Privacy-by-Default is mandatory for GDPR compliance**



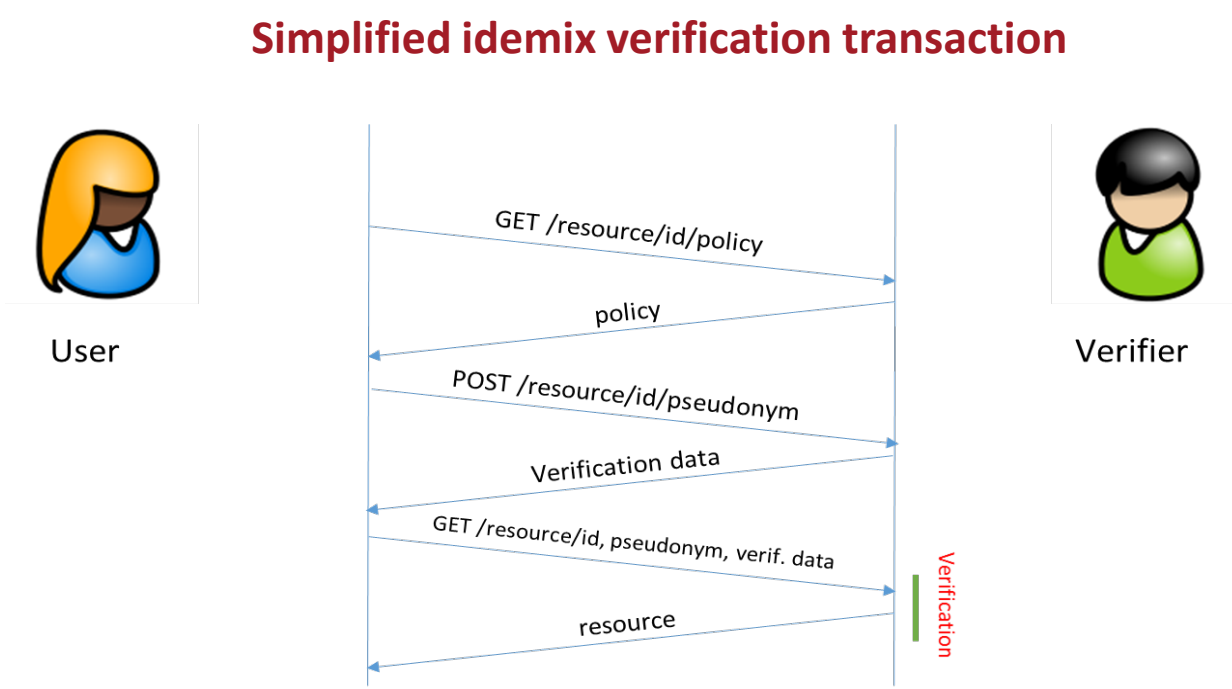
Privacy Preserving Attribute-Based Access Control (P-ABAC)

- **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

Anonymous access



Simplified idemix issuance transaction



Simplified idemix verification transaction

26869985631682372253256636408348855575464066578229061409826643921100627574884, 71763482699009900325890556718198150781635771, 2277101537980267232110591, 83004707837211581991, 23490470611349108

These attributes have no meaning by themselves

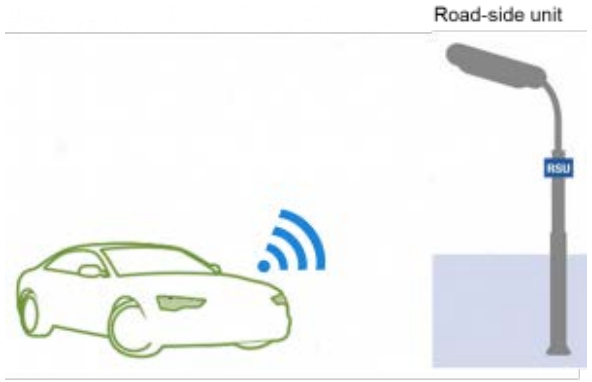
ReCRED's Innovation

- **Standardized** and **secure** authentication using **FIDO**
  - **FIDO protocol implementation**
- **Multifactor** & **easy to use password-less** authentication
  - Both **biometrics** and **behavioral** authentication
- **Security-by-design** by employing the **crypto functions** and **secure storage** of **TEE**
  - Implementation of **secure world applications** with **C programming language**
- **Identity Consolidator** as a **trusted registry** which offers
  - Identity **federation** & **management**, **user consent**, as well as reliable **failure recovery**
- **Privacy-by-design** of **online identities** using **anonymous credentials**
  - **Idemix** and **U-Prove** implementation
  - **Attribute-based Access Control policies**

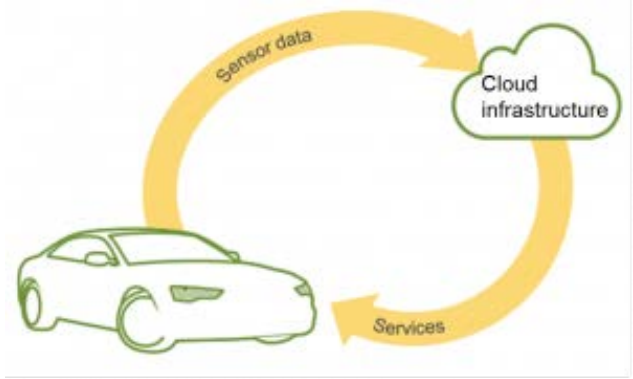
Current H2020 R&D projects

- **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/



Connected-vehicle system
Instance 1



Connected-vehicle system
Instance 2

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.

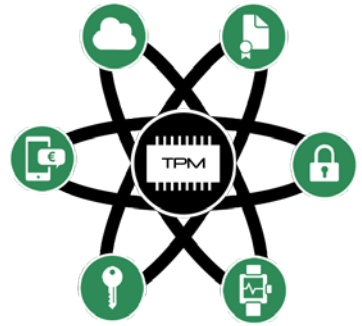
- **UPRC is responsible for designing and implementing Single Sign solutions with Attribute Based Access Control (ABAC)**

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

- **SealedGRID:** Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID *(H2020-MSCA-RISE-2017)*
- **Mission**
  - Aims at developing and implementing a scalable, highly trusted, and interoperable Smart Grid security platform.
- **Approach**
  - It will design and implement an innovative platform of high and state-of-the-art security methodologies, such as:
    - Key Management
    - Encryption
    - Signature
    - Blockchain
    - Attribute-Based Authorization Policy
    - Remote Attestation Mechanism

- **UPRC is the coordinator**

Sealed GRID

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων
ΓΓΕΤ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΕΥΔΕ ΕΤΑΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- **CityZEN :** Ολοκληρωμένο σύστημα διαχείρισης υποδομών και παροχής υπηρεσιών IoT για την έξυπνη πόλη *(T1ΕΔΚ-02121)*

- **NETPHISH:** Ανάπτυξη καινοτόμου εργαλείου τελικού χρήστη για την προστασία από επιθέσεις ηλεκτρονικού "ψαρέματος“ *(T1ΕΔΚ-05112)*

- **Re-cent:** Ολοκληρωμένη υπηρεσία διαμοιρασμού δικτυακών πόρων για την εξατομικευμένη διανομή ψηφιακού περιεχομένου σε δίκτυα δεδομένων 5ης γενιάς *(T1ΕΔΚ-03524)*

Project that will start on Jan 2019

CUREX: Secure and Private Health Data Exchange *(SU-TDS-02-2018)*

INCOGNITO: Identity verification with privacy-preserving credentials for anonymous access to online services *(H2020-MSCA-RISE-2018)*

SECONDO: A security economics service platform for smart security investments and cyber insurance pricing in the beyond 2020 networking era *(H2020-MSCA-RISE-2018)*

Recently developed tools:

- **Commix: Detecting and exploiting command injection flaws** https://github.com/stasinopoulos/commix *Presented in Black Hat 2015 Europe, Included in the latest version of Kali Linux.*

- **ROPInjector: Using Return Oriented Programming for Polymorphism and Antivirus Evasion.** https://github.com/gpoulios/ROPInjector, *Presented in Black Hat 2015, USA.*

- **(U)SimMonitor: A Mobile Application for Security Evaluation of Cellular Networks,** https://github.com/SSL-Unipi/U-SIMonitor *Presented in CyCon 2015, Estonia, Presented in Computers & Security, Elsevier Science, Vol. 60, Issue 1, pp: 62-70, July 2016*

Visit our website at www.ds.unipi.gr/security/

Follow us on  @SSLUNIPI

UNIVERSITY OF PIRAEUS

UNIVERSITY OF PIRAEUS RESEARCH CENTER