EU Threat Landscape
Threat Analysis in Research
ENISA Workshop
Brussels 24th February 2015

Aristotelis Tzafalias
Trust and Security Unit H.4
DG Connect
European Commission

Trust and Security: One Mission

- Develop policy, research and innovation solutions and carry out activities **enhancing the security of Internet networks and services** and the **protection of citizens' on-line privacy and security**.

Agenda

- A few examples from research.
- Overview of Security and Privacy in H2020
- "Information driven Cyber Security Management"

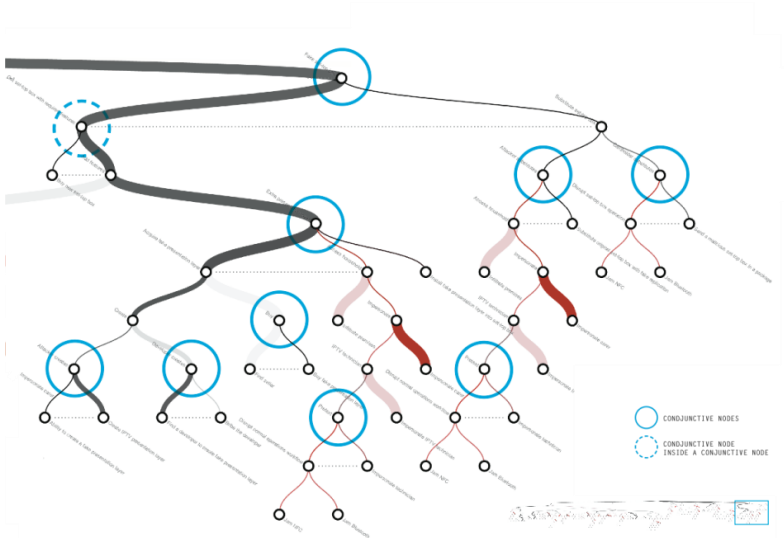
European Commission

predict
prioritise
prevent

TREsPASS

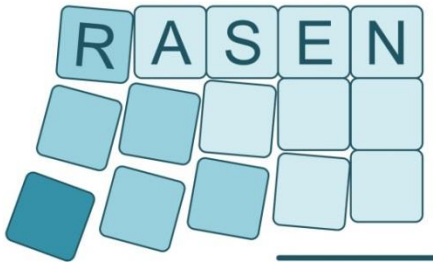
www.trespass-project.eu
@TREsPASSProject

Do you know the threat you face from different kinds of attackers? We do! The TREsPASS project develops security analyses that:



- Separate system model (difficulty) and attacker model (threat capability), based on FAIR taxonomy;
- Enable model checking the system to prioritise attacks/controls;
- Reconcile technical attacks and social engineering.

European Commission



Compositional Risk Assessment and Security Testing of Networked Systems

RASEN develops a method and toolbox that

- **Uses risk-based security testing to identify cybersecurity threats at a technical level**
- **Enables technical cyber threats to be assessed and prioritized in terms of impact on risk and business level assets**
- **Uses cyber security threat profiles to guide risk assessment and security testing**
- **Combines legal compliance and risk assessment to ensure compliance with standards and regulations for cybersecurity**

NECOMA

NECOMA

Threat data collection (WP1): gathering of information related to security from both client and infrastructure points of view

Threat data analysis (WP2): APIs, tools and platform for security-oriented data analysis

Cyber-defense for resilience (WP3): tools and demonstrators leveraging data analysis for threat mitigation

http://www.necoma-project.eu/
http://www.necoma-project.jp/

CUMULUS Project

- CUMULUS supports continuous and automated cloud service certification based on combinations of test, monitoring and TPM evidence, as well as combinations of them
- CUMULUS certification is based on executable evidence collection & assessment models (certification models)
- CUMULUS can assess the effectiveness of mechanisms implemented to mitigate threats. Examples of such threats include:
  - Web application threats – Particularly those arising from some types of SQL injection attacks (e.g., use of escape characters, incorrect type handling)
  - Data breaches – Particularly those arising from incorrect user authentication, tampering and database errors
  - Identity theft – Particularly those arising from id passing across applications

http://www.trescca.eu

- *Reference architecture of trustworthy cloud client with enhanced HW and SW security*
  - **Virtualization based isolation of trusted and non-trusted applications on *smart* devices**
  - **HW supported *Trusted Execution Environment* for security sensitive application**
- *Secure hardware for security software*
- *High grade protection against physical attacks, untrusted software and malware*

Confidential and Compliance clouds

- Design a confidential and compliant cloud for Europe allowing cloud users to securely and privately share their data in a cloud environment, among the users across the cloud and mobile devices.

- Provide a trust infrastructure enabling the data protection against data breaches, information leakage and cyber espionage, directly built on data.

- The project delivers:
  - ✓ a secure end-to-end data sharing infrastructure from data repository to user device (mobile or fixed) and vice-versa;
  - ✓ a data sharing agreements authoring tool, with legal and business compliance ensured by design, leveraging on predefined ontologies;
  - ✓ an approach to define data sharing policies in natural language;
  - ✓ ”hot-topic test bed”: three pilots from unrelated domains (healthcare, eGovernment and firm’s mobile devices scenarios).

- Secure and private data sharing will increase user trust in cloud services and ultimately increase the widespread adoption of cloud computing. Greater use of cloud computing will have benefits for users and for the digital economy in general.

Site: http://www.coco-cloud.eu/ twitter.com/CocoCloud_FP7

Attribute-based Credentials for Trust

- *ABC4Trust has designed, implemented, and trialled an Architecture for Privacy-preserving Attribute-based Credentials (Privacy-ABCs).*

- *Privacy-ABCs offer **Strong Authentication** that can prevent **Identity Theft/Fraud.***

- *Privacy-ABCs enable **Minimal Disclosure***
  - allowing users to limit the revealed identity information to the minimum set that is needed to access the resources and therefore avoid unwanted **Information Leakage** and **Spam**;
  - allowing service providers to reduce their unnecessary personal data collected from users and consequently reduce the risk of **Data Breaches**.

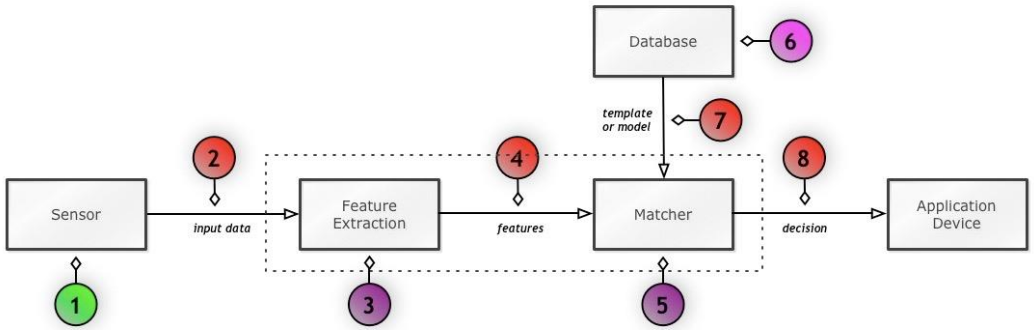
Website: https://abc4trust.eu

Video Clip: https://abc4trust.eu/download/Clip/ABC4Trust.mp4

TABULA RASA - Trusted Biometrics under Spoofing Attacks

Conventional biometric systems are vulnerable to direct (spoofing) attacks at the sensor level

http://www.tabularasa-euproject.org



- evaluations on the vulnerabilities of biometric systems
- countermeasures to spoofing attacks
- databases of spoofing attacks
- anti-spoofing solutions integrated into working systems
- standards on anti-spoofing technologies

European Commission

CLOUD ACCOUNTABILITY PROJECT

- *A few points from the Threats Landscape Report:*
  - **"Sloppiness … number one reason for breaches"**
  - **"Unknown number of breaches and incidents is a major concern"**
  - **"Concern regarding Cloud … complexity, flexibility"**
- *Focus on threats and on SIEM is not enough*
- *Must adopt a holistic approach for strong accountability*
  - **Accepting all responsibilities (law, agreement, ethics)**
  - **Addressing organizations, processes and technologies**
  - **Working across the cloud supply chain**
  - **Reporting transparently, being responsive and offering remediation**
- *The Cloud Accountability Project investigates accountability for ethical governance and stewardship of personal data within cloud environments*

European Commission

HINT Holistic Approaches for Integrity of ICT-Systems

http://www.hint-project.eu/

2 novel methods for testing **Hardware Trust**

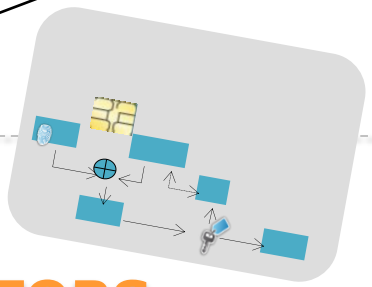
PUF Technology

DEVICE AUTHENTICATION

Side Channel Analysis for Hardware Trojan detection

DEVICE INTEGRITY

Professional Mobile Radios



Smart Cards

USE CASES & DEMONSTRATORS

Related threats: Hardware Trojans, Information leakage, Identity fraud (impersonation), Cyber espionage, Counterfeiting

A Network of Excellence in Systems Security

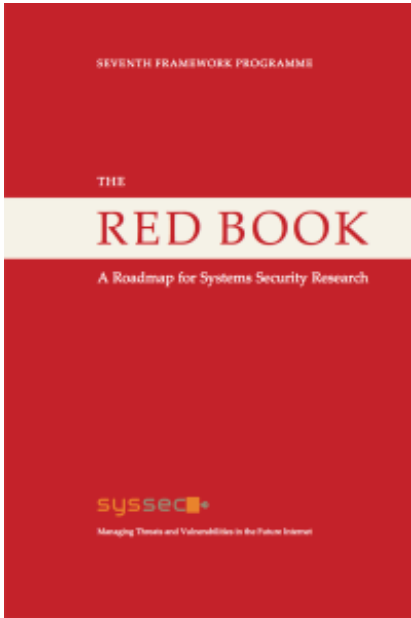
The Red Book: A Roadmap in Cybersecurity Research

"What if" Questions:

- What if there is no death for our data?
- What if there is no malware?
- What if 50% of the computers are compromised?
- What if there is no Internet? (for a day or two)

Grand Challenges:

- No device should be compromisable
- Give users control of their data
- Provide private moments in public places
- Develop compromise-tolerant systems



CYSPA: European Cyber Security Protection Alliance

- Creation of a CYSPA Core Alliance (global approach) to better tackle cyber risks in critical infrastructures, gathering demand and supply, consolidating sectoral and national needs
- Improve awareness of decision makers, use common risk management methodologies, share best practices, build a common trust platform in each main sector (vertical approach) -> CYSPA risk tool
- Impact reports describing the threats and agents landscape for each sector
- CYSPA eGov Impact report
- CYSPA Energy Impact report
- CYSPA Finance Impact report
- CYSPA Transport Impact report

@CYSPA_Project

www.cyspa.eu

CYSPA
EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

Crawling the web for vulnerabilities strews.eu

- Web landscape report on assets
  - SQL injection is solved, but not dead yet
  - Cross-site scripting is coming massively – consider participating in solutions in W3C WebAppSec WG
- W3C and IAB Workshop on pervasive monitoring in London (Feb 2014)
  - Vancouver IETF plenary concluded that Pervasive Monitoring (PM) represents an attack on the Internet.
  - Encrypt as much as you can
  - Tor works

STREWS

SEVENTH FRAMEWORK PROGRAMME

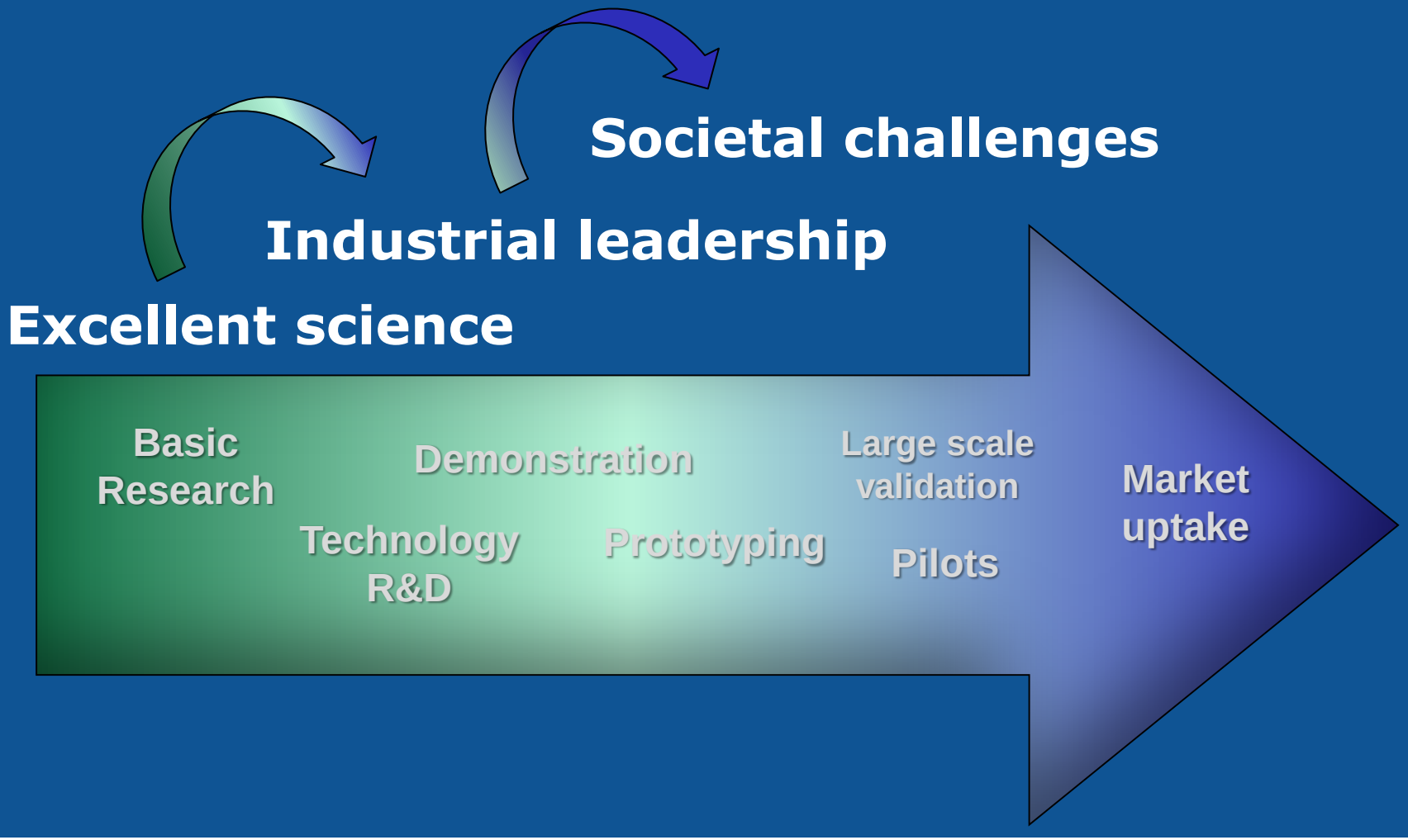
THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020

Three Pillars

€70 bn

Coverage of the full innovation chain



Policy Driven

Finance, Banking, Payment

Smart Cities

Connected Cars

Smart Grids

Intelligent Transport Systems

eHealth mHealth

Securing Present & Future Critical Market Functions

Mainstreaming Cybersecurity

Technology Driven

IoT

Big Data

Cloud

5G

Embedded Systems

Computing

Securing Data Processing, Storage and Transmission

H2020 SC7 Secure societies - Four key concepts

- Secure societies – Protecting freedom and security of Europe and its citizens.
- Address the economic and societal dimension of security and privacy in the digital ecosystem.
- Secure and increase trust in the digital society.
- Demonstrate the viability and maturity of state-of-the-art solutions.

Four Topics in 2015

- DS-03-2015: The role of ICT in Critical Infrastructure Protection (IA)
- **DS-04-2015: Information driven Cyber Security Management (IA)**
- DS-05-2015: Trust eServices (IA)
- DS-07-2015: Value-sensitive technological innovation in Cybersecurity (CSA)

Information driven Cyber Security Management

- **Challenge:**
  - Effective defence against […] threats requires the addition of a balancing, outward focused approach, on understanding the adversary's behaviour, capability, and intent.
  - Those […] responsible for managing cyber security programmes are often faced with an overwhelming amount of information, often raw and unstructured […]
  - SMEs face a particular challenge […] they often do not have the capacity […] or the […] expertise […] in order to address the cyber security threats they face.
  - […]
- **Scope:**
  - […] tools and techniques that enable organisations to efficiently process the flow of information from both internal and external sources, through improved information processing, analysis and, where necessary, exchange.

Information driven Cyber Security Management

- **Scope (cont.):**
  - […] should leverage the state-of-the-art in areas such as SIEM, data analytics (including Big Data) and visualisation, threat intelligence, malware analysis and cyber security information exchange.
  - […] promote interoperability through the use of globally accepted open standards and wider uptake of any proposed solutions.
  - […] address the needs of those entities whose mission it is to assist others such as […] Cyber Security Centres or similar.
- **Impact:**
  - […] effective vulnerability remediation, enhanced prevention and detection capabilities and faster response to incidents.
  - […] increase the level of awareness and preparedness.

Budget and schedule

- Call identifier: H2020-DS-2015-1
- Topic: DS-5-2015
- Instrument: Innovation Action (TRL 6 - Technology demonstrated in relevant environment)

- Indicative budget: 14,31 million EURO
- Indicative project size: 3-5 million EURO

- Opening date: 25/03/2015
- Deadline: 27 August 2015, 17.00.00 CET

Cybersecurity & Privacy Innovation Forum 2015

- 28-29th April 2015
- Venue: MCE, Brussels
- This event will include DG CNECT informational sessions relating to 'Digital Security: Cybersecurity, Privacy & Trust' calls in 2015
  - **DS-03-2015,DS-04-2015,DS-05-2015, DS-07-2015.**
    - *https://www.cspforum.eu/2015*

CNECT-TRUST-SECURITY@ec.europa.eu

Aristotelis.Tzafalias@ec.europa.eu

@EU_TrustSec

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2015-1.html