Digital Security

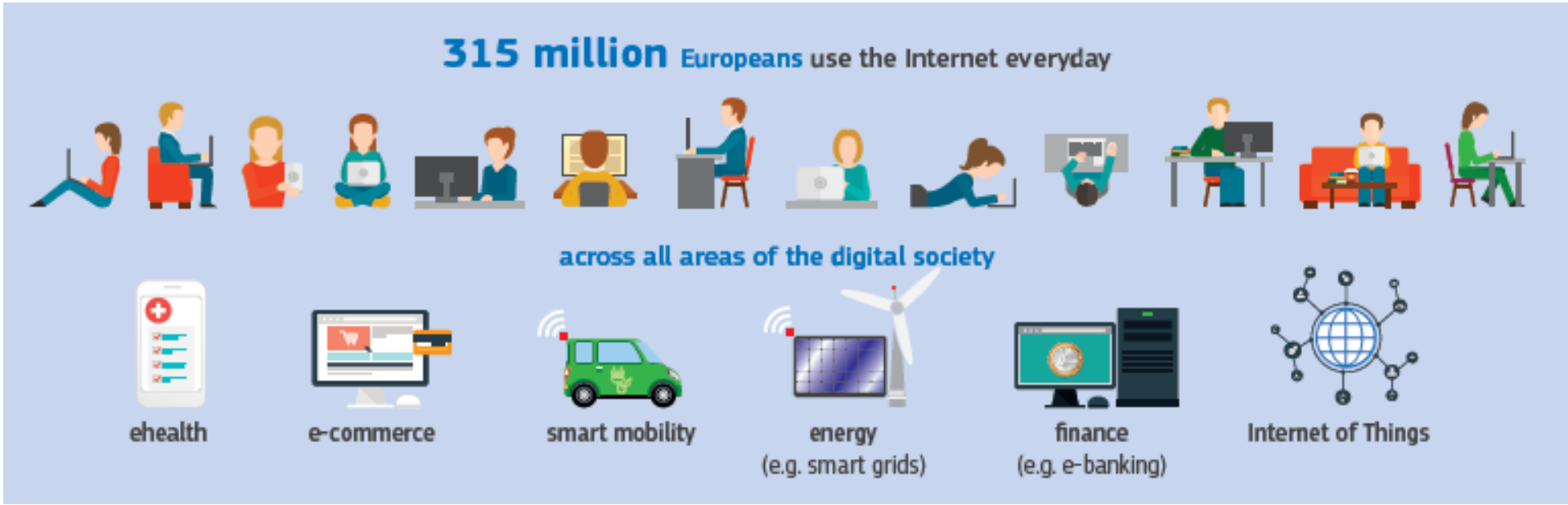
Rafael Tesoro Carretero
DG CNECT, Unit H1 - Cybersecurity & Digital Privacy

Contents

- Introduction
- Grants - Call for proposals in Digital Security
- Horizon Prize - Online seamless authentication
- Other related topics

Introduction

Cyberspace: a backbone of digital society & economic growth



European Commission

Cybersecurity incidents are increasing at an alarming pace with potentially profound effect on daily functioning of society & economy, both online and offline

Cybersecurity incidents may

disrupt the supply of essential services such as

water, healthcare, electricity or mobile services

Undermine trust in digital services & products

only 22% of Europeans

have **full trust** in companies such as **search engines**, **social networking** sites & **e-mail** services

Only 38% of Europeans feel

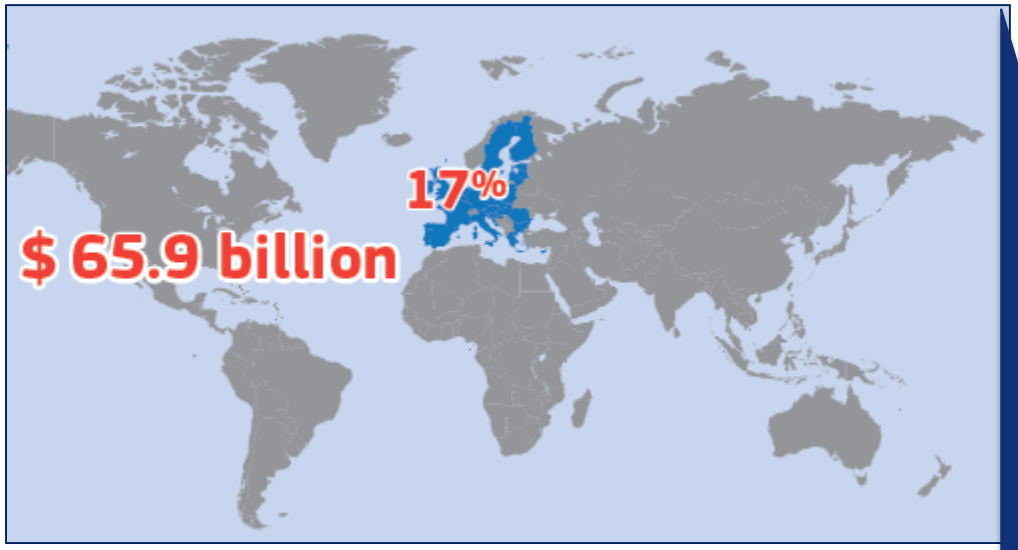
confident about **online purchasing** from **another EU Member State**

…as well as financial theft, loss of intellectual property, data breaches, etc.

What does this mean in practice?

The survival of strong European cybersecurity industry all together is at stake!

Cybersecurity is also an opportunity!



TODAY

TOMORROW

*The **global cyber security market** is expected to be among the **fastest growing** segments of the ICT sector in the coming decade. It is expected to **grow to $80-120 billion** by 2018.*

European Commission

Cybersecurity contractual Public-Private Partnership (cPPP)

- Stimulate the **competitiveness and innovation** capacities of the digital security and privacy industry in Europe
- Ensure a sustained **supply of innovative cybersecurity products and services** in Europe

European Commission

- **H2020 = legal framework** for the establishment of the cPPP
- **H2020 LEIT-ICT** to focus on technology-driven digital security building blocks and horizontal requirements
- **H2020 Societal Challenge 'Secure Societies'** to deliver societal benefits for users of technologies (citizens, SMEs, critical infrastructures…).
- **H2020 public funds to be matched by private sector investment**

European Commission

Call for proposals in Digital Security

Call – Digital Security Focus Area – Topics

- DS-06-2017: Cybersecurity PPP: **Cryptography**
- DS-07-2017: Cybersecurity PPP: **Addressing Advanced Cyber Security Threats and Threat Actors**
- DS-08-2017: Cybersecurity PPP: **Privacy, Data Protection, Digital Identities**

European Commission

SW4gbGluZSB3aXRoIHRlY2hub2xvZ2ljYWwgZGV
2ZWxvcG1lbnRzIGFuZCBlbWVyZ2luZyB0aHJlYXR
zLCB0aGUgaW1wcm92ZW1lbnQgb2YgcGVyZm9y
bWFuY2UgYW5kIGVmZmljaWVuY3kgb2YgY3J5cH
RvZ3JhcGhpYyBzb2x1dGlvbnMgaXMgYSBwZXJza
XN0ZW50IG5lZWQgYWNyb3NzIEIDVC4=

DS-06-2017: Cybersecurity PPP: Cryptography

European Commission

DS-06-2017: Cybersecurity PPP: Cryptography (RIA)

- *In line with technological developments and emerging threats, the improvement of performance and efficiency of cryptographic solutions is a persistent need across ICT.*

- Nine thematic research challenges, including:
  - Ultra-lightweight
  - High speed
  - Implementation
  - Authenticated encrypted tokens
- Increase trust in ICT and online services
- Protect the European Fundamental Rights of Privacy, Data Protection

European Commission

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

European Commission

DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors

- Situational Awareness (RIA);
  - Detect and quickly and effectively respond to sophisticated cyber-attacks;
  - Interdisciplinary research to counter threat actors and their methods;
  - Assess and address the impact to fundamental rights, data protection and privacy in particular;
- Simulation Environments, Training (IA);
  - Prepare those tasked with defending high-risk organisations;
  - Realistic environments; Tools for producing both benign and malicious system events;
  - May also address crisis management and decision making processes in relation to obligations stemming from applicable legal frameworks

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION
TITLE II – FREEDOMS

Article 6

Right to liberty and security

Everyone has the right to liberty and security of person.

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

European Commission

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities (IA)

- Privacy-enhancing Technologies (PET)
- General Data Protection Regulation in practice
- Secure digital identities
- Support for Fundamental Rights in Digital Society.
- Increased Trust and Confidence in the Digital Single Market
- Increase in the use of privacy-by-design principles in ICT systems and services

Call - DS – 2017 - Planning

Two separate opening dates - deadlines for submission		
Topic(s)	DS-06-2017	DS-07-2017 DS-08-2017
Opening	08 Dec 2016	01 Mar 2017
Deadline	25 Apr 2017	24 Aug 2017

Topic	Instr.	Funding (M)
DS-06-2016	RIA	20.50
DS-07-2016	RIA	10.0
	IA	8.0
DS-08-2016	IA	17.6

European Commission

Horizon Prize – Online seamless authentication

What are inducement prizes?

- A novel funding instrument, different from e.g. grants (a usual way to co-fund research projects).
- Prize contests address technological and/or societal challenges.
- A target is specified through award criteria.
- The reward goes to the contestant who (first/best) reaches the target.

Why "Horizon prizes" matter?

- A way to induce and advance innovations for cutting-edge solutions to problems.
- Leverage research and innovation (R&I) investment from the private sector in a given direction.
- Simplification and outcome orientation, as only the outputs from the contestants are evaluated.
- Entrepreneurship: Reduce barriers to participation compared with traditional instruments.

- *Passwords are a daily burden for online users*
- *Password security can be compromised by*
  - Being guessed,
  - brute force attack, or
  - data breach.

European Commission

- *Multi-factor authentication*
- *Concerns:*
  - Can be convoluted for the user
  - Need to have at hand another hardware gadget in addition to the main one used for the transaction

- *Biometrics are more convenient than passwords and multi-factor authentication methods.*
- *Concerns with biometrics:*
  - Lack of revocability after being spoofed.
  - When reliable, they require costly hardware infrastructure
  - Might be privacy intrusive

Expected results in seamless authentication prize

An information and communication technologies (ICT) solution that enables citizens to seamless authenticate themselves across a wide range of applications and devices.

The solution should be easy to use, reliable, robust against cyber-attacks, privacy-friendly and compatible as well as affordable and open.

It should be ready to benefit a wide range of the EU population, from healthy to impaired citizens of all ages.

Essential award criteria (1 of 3)

- significant contribution by the contestant in development and/or integration.
- The solution is **usable, convenient and easily accessible** by a wide range of users hence requiring low effort to adopt it from both end-users and service providers.
- The solution is **reliable**, satisfying high rates of accuracy for correctly authenticating users.
- The solution is **secure, robust and resilient** against state-of-the-knowledge cyber-attacks.

Essential award criteria (2 of 3)

- The solution takes into account the **privacy and data protection principles**.
- The solution is
  - **applicable**, working across a relevant collection of applications (including, but not limited to: social networks, email services, messaging services, online banking,…)
  - **compatible**, working across a relevant set of hardware devices and of operating systems
  - **affordable** for deployment in large scale and **cost-effective**, requiring low implementation and infrastructure costs for service provides and for end users.

Essential award criteria (3 of 3)

- The solution is **open**. The extent of open source software included in the solution should be maximum, in order to facilitate (a) its further tailor and development and (b) the assessment of its fulfilment of the award criteria (robustness, privacy and data protection principles).

Indicative timetable and budget

Stages	Indicative period
Opening of the contest	**First quarter 2017**
Deadline for submission of application	**Third quarter 2018**
Evaluation and solutions demonstration	**Fourth quarter 2018**
Award of the prize	**Fourth quarter 2018**

Horizon Prize	Funding (M€)
Online Security- seamless authentication	4.0

European Commission

Other related topics

Where else to find cybersecurity and privacy R&D&I in H2020?

Everywhere!

change of mindset

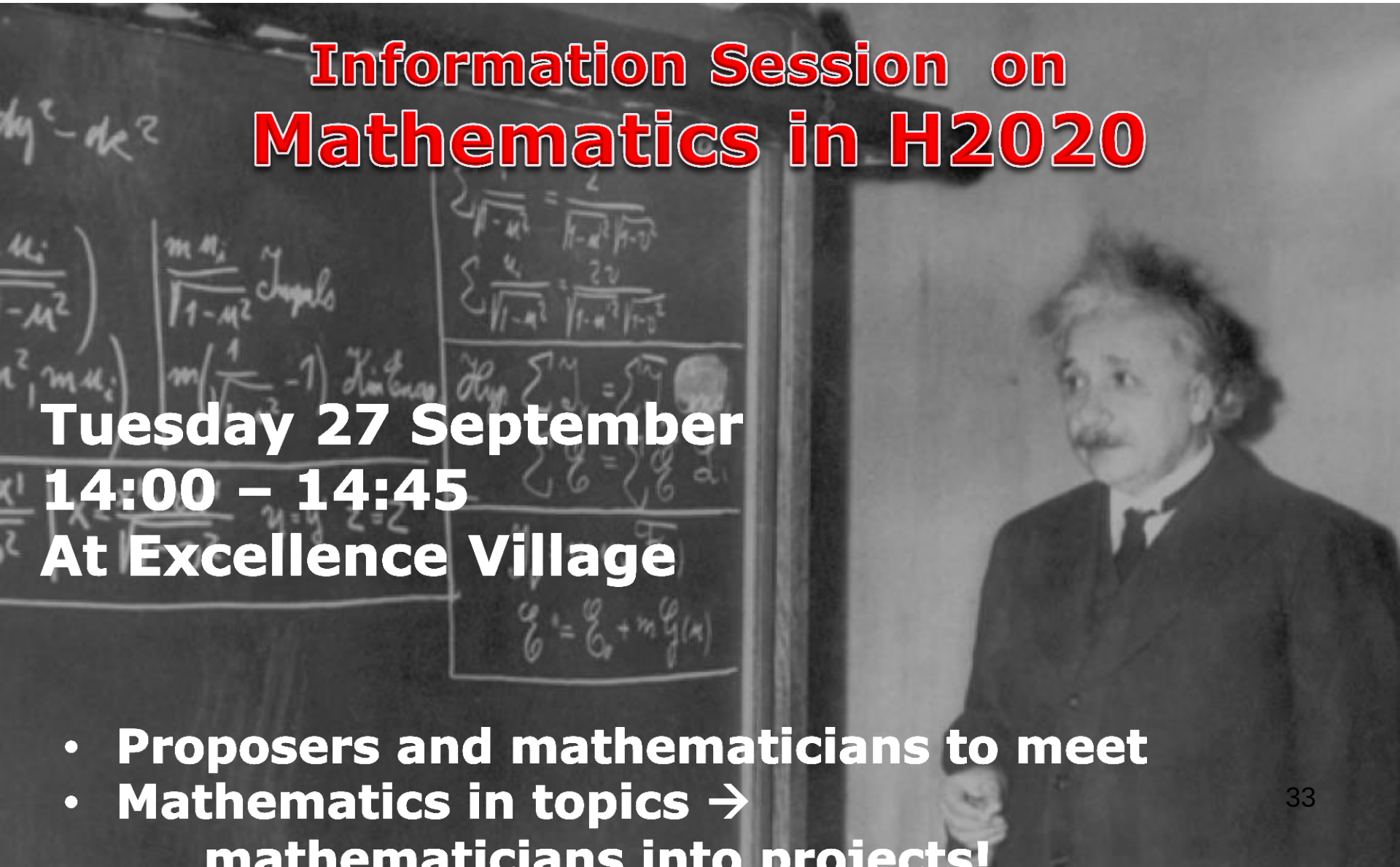
Examples of related topics

- CIP-01-2016-2017 : Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

- SMEinst-13-2016-2017 : Engaging SMEs in security research and development

European Commission

Information Session on Mathematics in H2020



Tuesday 27 September
14:00 – 14:45
At Excellence Village

- **Proposers and mathematicians to meet**
- **Mathematics in topics →**
  mathematicians into projects!

European Commission

Information Session on Mathematics

- **Why?**
  - **There is vast potential in the mathematical world in Europe**
  - **There is relevance for our WP topics**
  - **Proposals will have better quality with mathematical participation**
  - **We recommend mathematicians to be active**
  - **We recommend partners to talk with mathematicians**

References and support (1 of 2)

Work programme 2016-2017:

Secure societies – Protecting freedom and security of Europe and its citizens

http://europa.eu/!BG38Bf

National Contact Points (NCPs)

http://europa.eu/!up97Wv

- Guidance on choosing relevant H2020 topics and types of action
- Advice on administrative procedures and contractual issues
- Training and assistance on proposal writing
- Distribution of documentation (forms, guidelines, manuals etc.)
- Assistance in partner search

European Commission

References and support (2 of 2)

Work programme 2016-2017:

5.i. Information and Communication Technologies

Inducement prize: Online security - Seamless personal authentication

http://europa.eu/!RX49uX

Follow us in Twitter **@EU_TrustSec**

CNECT-H1@ec.europa.eu

European Commission

EXTRA SLIDES BEYOND THIS POINT

Cyber Attacks - recent examples

Bundestag: servers infected with malware

-> rebuilding of nearly all IT systems

TALKTALK: "significant cyber-attack" -> 4+ million customers' data potentially accessed

TalkTalk

European Commission

Key EU Objectives and Actions

Increase capabilities & cooperation	NIS Directive - NIS platform – ENISA - CEF
Strengthen EU Cybersecurity industry	Strengthening industrial capabilities– cPPP - 450M in H2020
Mainstream cybersecurity in EU policy	Cooperation on new policy initiatives – Sectorial cybersecurity strategies

Cyberspace is borderless by nature...

unlike heavily fragmented European market for ICT security products & services due to:

- **Dependence on public procurement & government purchase**
- **Lack of interoperability solutions, practices and well-functioning mechanisms of certification**
- **Different NIS policies across MS (to be addressed by the NIS directive)**
- **Barriers of trust for cross-border purchase**

European Commission

Objectives of the cPPP

Gather industrial and public resources to deliver innovation against a jointly-agreed strategic research and innovation roadmap.

Maximize available funds through better coordination with MS.

Focus on a few technical priorities defined jointly with industry.

Seek synergies to develop common, sector-neutral technological building blocks with maximum replication potential

Obtain economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities.

Be a platform to discuss other supporting measures for the industry