Mirjam Wester—Ed. (UEDIN)
Panos Louridas (GRNET)
Benjamin Weggenmann (SAP)
Harry Halpin (GH)

Dissemination Report III

Deliverable D2.10

January 31, 2019
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Dissemination Level: Public

Revision History

Revision	Date	Author(s)	Description
0.1	2018-01-23	MW (UEDIN)	Initial draft
0.2	2018-05-01	MW (UEDIN)	Intermediate draft- incorporating partners' dissemination activities
0.3	2018-11-22	RG (KUL)	Fill in missing details from KUL activities
0.4	2018-12-03	PL (GRNET)	e-Voting target groups
0.5	2018-12-04	MW (UEDIN)	Final draft - incorporating all partners' remaining dissemination activities
0.6	2018-12-04	MZ (UT)	Review and proofreading
0.7	2018-12-13	BW (SAP)	SAP target groups
0.8	2018-12-28	MW (UEDIN)	Draft submitted to EC
0.9	2019-01-08	HH (GH)	Messaging target groups
1.0	2019-01-31	MW (UEDIN)	Final version submitted to EC

Executive Summary

This dissemination report, the third of three, encompasses the dissemination activities of the project partners for the time period from September 2017 through to January 2019. Activities such as web-site, publications, conference visits and industry events are reported. In summary, all of the targeted dissemination channels were utilized with all hitting and some even surpassing the targeted number of outputs.

Contents

1. Introduction

This chapter states the purpose of the Dissemination Report of the final year and its relationship to other project deliverables.

1.1 Purpose of document

This report captures the dissemination activities of the PANORAMIX project partners from September 2017 through to January 2019. It enumerates the different activities according to the channels that were identified and described in the dissemination plan (D2.2). It also provides a comparison of key performance indicators against actual dissemination achievements.

1.2 Relation to other project deliverables

This document is a deliverable (D2.10) for Work Package 2 - "Dissemination" (WP2). It is a public document which will be made available on the project website for those stakeholders interested in the dissemination plan of the PANORAMIX project. This document covers the consortium's interaction with its external audience. Dissemination is applicable to all work packages (WPs) supporting the knowledge transfer from the consortium to the target audiences. This is especially important when considering the exploitation (Task 2.3) and standardization activities (Task 2.2). In particular, D2.10 is closely related to the following WP2 deliverables:

- D2.1 - Public Web Page and Blog [UEDIN]
- D2.2 - Dissemination plan [KUL]
- D2.3 - Dissemination Report I [KUL]
- D2.4 - Standardization Report [GH]
- D2.5 - Preliminary Exploitation Plan [SAP]
- D2.6 - Complete Exploitation Plan [GRNET]
- D2.7 - Report on Exploitation Activities and Updated Plan for Further Exploitation [GH, CCT]
- D2.8 - Scientific Advisory Board Reports [UT]
- D2.9 - Dissemination Report II [UEDIN]

2. Target groups per use-case

In this section, we explain in more detail how target groups for the different use cases have specifically been targeted and will continue to be engaged with beyond the lifetime of PANORAMIX.

2.1 e-Voting

GRNET has actively been promoting the results of the PANORAMIX project through its incorporation in the Zeus e-voting application. This mainly involves the following target groups:

1. Voting constituencies and electoral authorities.
2. Researchers and practitioners in e-voting applications.

Regarding the first group, the Zeus e-voting application is already in use and has been refactored to incorporate the research results of the PANORAMIX framework. Based on experiences with the users of the system, GRNET found that different mixnets, and different cryptographic settings, are suitable for different situations. For example, for a small-scale election, a slow but easy to understand mixnet, such as a Sako-Kilian one, is convenient and very appealing. For large scale elections, more advanced mixnets, such as those developed in the context of WP2, or externally developed mixnets such as Verificatum, are more suitable. A major promotion point of Zeus and PANORAMIX will be that, during election setup, the election administrators will be able to select among a set of alternatives. Moreover, this selection will be the result of a negotiation process, which will produce a cryptographically binding document with the results of the negotiation.

Moreover, to promote dissemination, the Zeus team will be working on:

- Internationalisation and localisation of Zeus, so that it can be adopted by more countries. A first step has been the localisation of Zeus in Romanian, used for the internal elections of the Save Romania Union (https://en.wikipedia.org/wiki/Save_Romania_Union) party for the appointment of its candidates for the coming European Parliament elections of spring 2018. Discussions have also taken place with developers in Uruguay for a Spanish language version.

- Dissemination of Zeus in particular user groups. Certain constituencies have specific voting requirements (in terms of the voting procedure and setup). For example, Zeus has teemed with a private company in the legal sector to provide support for the use of Zeus among lawyers, judges, and other law practitioners.

Regarding the second group, researchers and practitioners in e-voting applications, Zeus has been in discussions with the Verificatum mixnet (https://www.verificatum.org/). The Verificatum mixnet itself will be incorporated into Zeus, along with mixnets developed by Zeus partners. As Verificatum is a major mixnet initiative whose development was completely separate from Zeus, the interoperation of Zeus and Verificatum will serve as proof of validity of the overall Zeus and PANORAMIX architecture. Moreover, potential users that are already familiar will Verificatum will appreciate its interoperability with Zeus.

2.2 Surveys/Statistics

SAP's target groups for dissemination activities consist of mainly internal, but also external stakeholders.

Internal stakeholders Internal stakeholders are our main target and primarily consist of product development units within SAP that could benefit from PANORAMIX results and technology. Dissemination activities aimed at these internal stakeholders are hence closely related to our exploitation activities (cf. our exploitation plan and activities described in D2.7).

To reach these development units, we follow several approaches:

1. To reach a broad audience and potentially new stakeholders within SAP, we participate in SAP's own industry events which take place regularly throughout the year at specific locations in Europe and even world-wide. They range from specialized events such as the *SAP Security Summit* which specifically targets a security-focused community to diverse global events such as *SAP d-kom* and *SAP TechEd* that attract thousands of SAP employees as well as external visitors and customers. As such, these events provide a prominent platform to promote our work and project results to a considerable number of people.

2. If we know that specific product units could benefit from PANORAMIX technology, we contact them directly to discuss potential applications in their solutions. For instance, the *SAP HANA Core* and *SAP Security Transfer* teams are mainly working on data anonymization use cases themselves, and hence they clearly have a high chance of benefitting from PANORAMIX results. Therefore, we are in direct contact with them through a series of meetings to discuss potential topics for technology transfer.

3. Furthermore, we participate in internal information sessions to present our work and PANORAMIX technology to interested audiences. These are typically organized regular events that invite speakers to promote innovative ideas in general or to address specific topics such as security, and hence address target groups interested in those topics.

External stakeholders We also target external stakeholders for our dissemination activities.

As mentioned above, our industry events also attract external visitors and customers. This allows us to demonstrate available privacy-enhancing technologies that could help them implement their business cases, and hence create demand for technology transfer in our product development units also from the customer side.

Another important external target group is the academic community. We publish our own research in scientific conferences and journals and hence can get feedback for our work and exchange ideas by engaging researchers from all over the world. Moreover, this can lead to potential collaborations, for instance in upcoming EU research projects.

Furthermore, we also present our work and PANORAMIX results in university lectures and workshops. Again, this allows us to engage the academic community to discuss and exchange ideas. In addition to that, these activities allow us to reach students who pose another related target group and could draw their interest to do an internship or thesis at SAP, hence supporting a sustainable community around PANORAMIX-related topics.

2.3 Messaging

The messaging use-case target groups include a wide variety of early adopters of new privacy-enhancing technology, ranging from open-source advocates to members of civil society interested in privacy. Greenhost targets more end-users, while CCT is focussed more on the building of a developer community around the mix-net codebase itself.

- *End users*: In terms of the first target group, there has been considerable outreach to civil society and ordinary users interested in privacy. This has taken place primarily at events like Chaos Computer Congress and outreach events in countries, including ones that are normally not targetted such as Albania. These users were targetted for user-testing of the software, and for providing input on how easy the software was to install, whether it worked on their platforms of choice, the GUI, and the amount of delay that the mix-net caused. These users were also important to convey the ideas of PANORAMIX to a wider audience that may not have detailed technical knowledge, but a desire for privacy. These users form the core of the paying user-base of Greenhost, and so the outreach to these communities led to increased amount of Greenhost e-mail and VPN users.

- *Developers*: For the second target group, there has been even more outreach to open source developers to build a community around the project. This took place primarily at events such as Tor Developer Meetings and "hacker" gatherings such as BornHack, where open source developers were already congregating, in order to increase their interest in mix-nets. These meetings allowed CCT to recruit David Stainton and Aaron Gibson, and continuing attendance at these meetings allows new developers to be recruited to continue working on the software after the lifetime of the project. The outreach to these communities attracted enough attention from the open-source community to build a community of interest (over 30+ developers in IRC and following repositoires) and even media interest around the software.

There are also dissemination events outside these target groups that were relevant to the messaging use-case. In terms of building new kinds of target groups, we also tried to engage new communities that were not envisaged in the original Panoramix proposal. For example, we engaged the cryptocurrency community via attendance at events like HPCC and Bitcoin Wednesday. We also engaged new generations of academics by teaching courses at Ph.D. summer schools on mix-nets in conjunction with the E-CRYPT CSA, and also encouraged developers interested in mix-nets to interact with the academic community via attending the "Real World Crypto and Privacy" summer school. By building closer ties between open source developers and academia, the study and deployment of mix-nets for messaging is now on a much stronger foundation than it was before PANORAMIX began, creating a long-term growing community of both end-users and developers that have a mutually beneficial relationship with companies (Greenhost), non-profits (CCT), and academia.

3. Dissemination activities across different channels

This chapter describes all the dissemination activities across different channels. They follow the record format proposed in D2.2, emphasizing the relevance that each activity has to the project.

3.1 User-facing website articles, blog posts and twitter

The PANORAMIX twitter account https://twitter.com/PanoramixH2020 was created on 11/10/2016. It is used to bring attention to project highlights and key results by tweeting published papers, linking presentations and any other PANORAMIX news. The number of people following @PanoramixH2020 continues to grow, having reached more than 315 by January 2019.

Short descriptions of the blog posts published during Y3 are given in this section. The resources spent on writing the blog posts vary between 10-20 minutes per post. The number of people reached for the blog posts on panoramix-project.eu has stayed more or less consistent at around 200 sessions per month as Figure 3.1 shows.

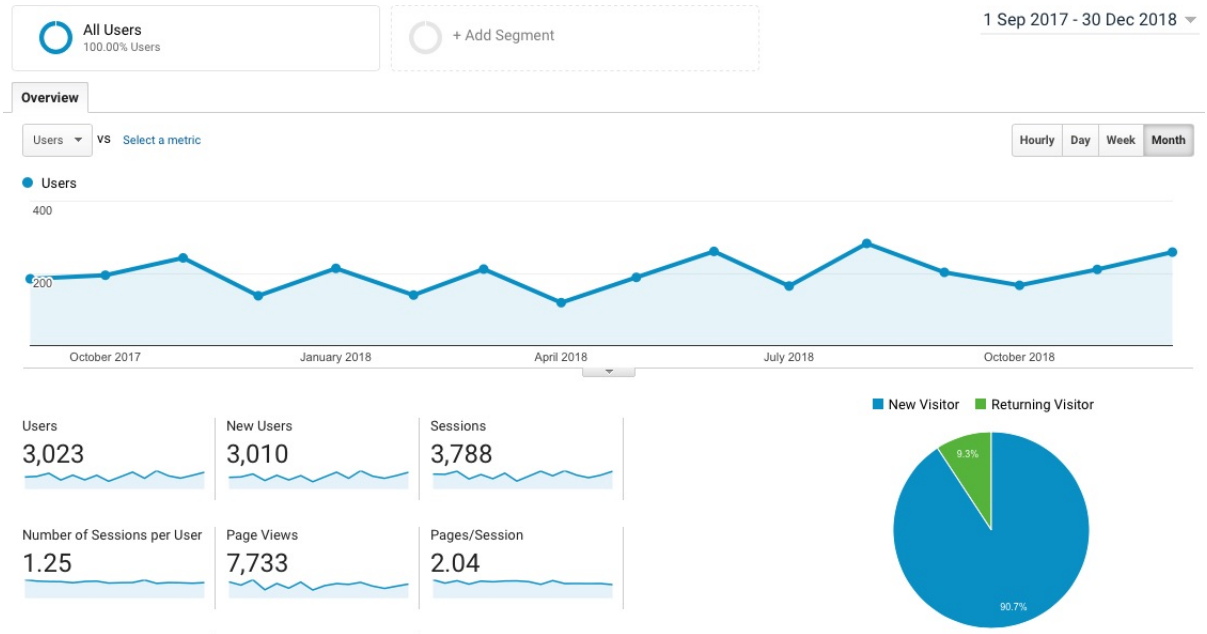

Figure 3.1: Analytics of the PANORAMIX website.

The following blog posts were published on the PANORAMIX website during Y3 of the project:

Title	PANORAMIX at Congreso de Privacidad (CDP) in Madrid 17-19 October
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-congreso-de-privacidad-cdp-in-madrid-17-19-october/
Date published	October 18, 2017
Partners involved	GRNET, Greenhost, KUL
People involved	Dimitris Mitroupoulos, Georgios Tsoukalas, Giorgos Korfiatis, Kali Kaneko, Meskio and Rafael Galvez
Relevance to the project	PANORAMIX took part in the H2020 joint dissemination activity at the European Privacy and Data Protection Summit co-organised by H2020 TYPES project, one of the other EU projects on privacy innovation.

Title	PANORAMIX at WPES (30 Oct 2017) and ACM CCS (30 Oct – 3 Nov 2017)
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-wpes-30-oct-2017-and-acm-ccs-30-oct-3-nov-2017/
Date published	November 6, 2017
Partners involved	UCL,
People involved	George Danezis, Ania Piotrowska,Vasilios Mavroudis and Claudia Diaz
Relevance to the project	Further dissemination of strong PANORAMIX presence at top tier cybersecurity conference.

Title	Katzenpost Hackathon December 2017
Type	Blog post
Location/URL	https://panoramix-project.eu/katzenpost-hackathon-december-2017/
Date published	February 2, 2018
Partners involved	CCT, Greenhost, GRNET
People involved	WP7/WP4 contributors.
Relevance to the project	News on progress in WP7.

Title	PANORAMIX Panel At CPDP 2018
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-panel-at-cpdp-2018/
Date published	February 7, 2018
Partners involved	UDIN, KUL
People involved	Aggelos Kiayias, Claudia Diaz
Relevance to the project	Blogpost to report on the CPDP panel organised by PANORAMIX.

Title	PANORAMIX at Project Clustering Workshop
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-project-clustering-workshop/
Date published	March 19, 2018
Partners involved	GRNET
People involved	Panos Louridas
Relevance to the project	Report on the H2020 clustering workshop with 25 H2020 projects.

Title	How Unique is Your .onion? Analysing of the Fingerprintability of Tor Onion Services
Type	Blog post
Location/URL	https://www.esat.kuleuven.be/cosic/how-unique-is-your-onion-analysing-of-the-fingerprintability-of-tor-onion-services/
Date published	April 5, 2018
Partners involved	KUL
People involved	Rebekah Overdorf
Relevance to the project	Advertising of a new PANORAMIX publication.

Title	PANORAMIX at PKC 2018
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-pkc-2018/
Date published	May 2, 2018
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Advertising of new PANORAMIX publication.

Title	PANORAMIX at SIGIR '18
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-sigir-18/
Date published	June 5, 2018
Partners involved	SAP
People involved	Benjamin Weggenmann, Florian Kerschbaum
Relevance to the project	Advertising of a new PANORAMIX publication.

Title	PANORAMIX Sponsors roundtable on e-voting for participatory budgeting
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-sponsors-roundtable-on-e-voting-for-participatory-budgeting/
Date published	June 9, 2018
Partners involved	KUL
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Spreading awareness of the roundtable.

Title	Round Table on electronic voting for participatory budgeting
Type	Blog post
Location/URL	https://panoramix-project.eu/round-table-on-electronic-voting-for-participatory-budgeting/
Date published	July 5, 2018
Partners involved	KUL
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	E-voting is one of the use cases in PANORAMIX, and this blog post reports on what was discussed.

Title	PANORAMIX releases project Katzenpost
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-releases-project-katzenpost/
Date published	November 13, 2018
Partners involved	CCT
People involved	Moritz Bartl
Relevance to the project	Announcement of the release of the mixnet for e-mail.

Title	Lecture at SAP TechEd 2018 in Bangalore, Friday November 30th
Type	Blog post
Location/URL	https://panoramix-project.eu/lecture-at-sap-teched-2018-in-bangalore-friday-november-30th/
Date published	November 26, 2018
Partners involved	SAP
People involved	Benjamin Weggenmann
Relevance to the project	Announcement of SAP dissemination activity.

3.2 Research Conference

This section lists the research conferences that PANORAMIX has been involved with during Y3. Research conferences are one of the main dissemination venues for the scientific research carried out in PANORAMIX. The target group reached at the conferences is the research and scientific community. All publications are listed on the PANORAMIX website https://panoramix-project.eu/conferences/ with links to their open access versions. Resources expended for

each paper are difficult to capture, as a rough ballpark estimate, between 0.05 and 0.1 PM per publication.

Title of conference	Workshop on Privacy in the Electronic (WPES) Society
Type	Conference presentation and publication
Title of publication	"AnNotify: A Private Notification Service" [PHG+17]
Location	Dallas, Texas
Date	30 October 2017
Partners involved	UCL
People involved	Ania Piotrowska, George Danezis
Relevance to the project	AnNotify presents a scalable service for private and low-cost notifications, which is based on mix-networks. Private notifications are important, since the fact that someone received a notification about an event, like a notification about an email, might already leak information. At WPES I presented the design of Anotify and discussed the security and efficiency with other members of the community.
People reached	40 people from the privacy, security and anonymous communication community, academics and industry

Title of conference	Workshop on Privacy in the Electronic Society (WPES)
Type	Conference presentation and publication
Title of publication	"Mix-ORAM: Using delegate shuffles" [TDE17]
Location	Dallas, Texas
Date	30 October 2017
Partners involved	UCL
People involved	George Danezis
Relevance to the project	Mix-ORAM presents four different designs inspired by mix-net technologies with reasonable periodic costs.
People reached	40 people from the privacy, security and anonymous communication community, academics and industry.

Title of conference	ACM Conference on Computer and Communications Security (CCS)
Type	Conference presentation and publication
Title of publication	"A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components" [MCS+17]
Location	Dallas, Texas
Date	30 October - 3 November 2017
Partners involved	UCL
People involved	Vasilios Mavroudis, George Danezis
Relevance to the project	This is the academic paper introducing our novel architecture for security and privacy sensitive devices and evaluating our prototype. Our prototype is capable of protecting crucial mixnodes from sophisticated fabrication-level attacks that aim to either leak secret keys or generate weak/backdoor-ed ones.
People reached	100 experts in hardware security and multiparty computations from both the academia and the industry.

Title of conference	"Living in the Iot" IET PETRAS Conference 2018
Type	Conference presentation and publication
Title of publication	"Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces" [MV18]
Location	London, UK
Date	30 October - 3 November 2017
Partners involved	UCL
People involved	Vasilios Mavroudis, Michael Veale
Relevance to the project	A survey paper shedding light on both the technical and the legal aspects of various modern tracking technologies.
People reached	200 experts in academia, government and industry.

Title of conference	ACM Conference on Computer and Communications Security (CCS)
Type	Conference presentation and publication
Title of publication	"How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services" [OJA+17]
Location	Dallas, Texas
Date	30 October - 3 November 2017
Partners involved	KUL
People involved	Marc Juarez, Rebekah Overdorf, Claudia Diaz
Relevance to the project	Measuring the level of protection of anonymous communications systems is critical for their adoption. Novel and powerful attacks can be carried out through the use of Machine Learning agents. This paper explains looks at what kind of features make these attacks successful in the particular case of anonymous websites, and also countermeasures can the designers of the website put in place.
People reached	200 people from academia and industry

Title of conference	Advances in Cryptology - 23nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2017)
Type	Conference presentation and publication
Title of publication	"An Efficient Pairing-Based Shuffle Argument" [FLSZ17]
Location	Hong Kong, China
Date	3 - 7 December 2017
Partners involved	UT
People involved	Helger Lipmaa, Janno Siim, Michał Zając
Relevance to the project	The paper proposed a new more efficient shuffle argument. Since shuffle arguments are usually the bottleneck of a (re-encryption) mix-net, any efficiency gain is of great importance for the general mix-net performance.
People reached	200 people mostly from academia

Title of conference	Advances in Cryptology - 23nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2017)
Type	Conference presentation and publication
Title of publication	"A Subversion-Resistant SNARK" [ABLZ17]
Location	Hong Kong, China
Date	3 - 7 December 2017
Partners involved	UT
People involved	Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, Michał Zając
Relevance to the project	The paper presents new techniques for obtaining subversion resistance. Subversion resistance for non-interactive zero knowledge proofs (as presented in the paper) allows prover to make a sound and private argument without necessity of a trusted third party. Thus it minimizes the trust assumptions one has to make to be able to use the argument.
People reached	200 people mostly from academia

Title of conference	The Network and Distributed System Security Symposium (NDSS 2018)
Type	Conference presentation and publication
Title of publication	"Inside Job: Applying Traffic Analysis to Measure Tor from Within" [JJG+18]
Location	San Diego, USA
Date	February 18-21, 2018
Partners involved	KUL
People involved	Marc Juarez, Rafael Galvez, Tariq Elahi, Claudia Diaz
Relevance to the project	This paper twists the traditional threat model of an anonymous communication system, and proposes a way to measure sensitive events in a privacy preserving way.
People reached	200 people from academia and industry

Title of conference	The Network and Distributed System Security Symposium (NDSS 2018)
Type	Conference presentation and publication
Title of publication	"Automated Website Fingerprinting through Deep Learning. " [RPJ+18]
Location	San Diego, USA
Date	February 18-21, 2018
Partners involved	KUL
People involved	Marc Juarez
Relevance to the project	State of the art attacks against anonymous communication systems are increasingly making use of recent breakthroughs in Machine Learning. Their success is directly related to the features used by the algorithms. This paper proposes a way to automatically extract them.
People reached	200 people from academia and industry

Title of conference	20th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC 2018)
Type	Conference presentation and publication
Title of publication	"Bootstrapping the Blockchain, with Applications to Consensus and Fast PKI Setup" [GKLP18]
Location	Rio de Janeiro, Brazil
Date	25 – 29 March 2018
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Specialised cryptography conference. Presentation of the paper to the cryptography community.
People reached	120 Research and scientific community

Title of conference	International Workshop on Privacy Engineering
Type	Conference presentation and publication
Title of publication	"The Odyssey: modeling privacy threats in a brave new world" [GG18]
Location	London, United Kingdom
Date	23-27 April 2018
Partners involved	KUL
People involved	Rafael Galvez
Relevance to the project	We presented The "Odyssey", a paper focused on the practicality of the analyzing privacy threats in the modern software development workflow. The exposure of this PANORAMIX paper and the consequent feedback is relevant to the further development of the PANORAMIX framework once the community takes the maintenance role.
People reached	30 people from academia and industry

Title of conference	37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018)
Type	Conference presentation and publication
Title of publication	"Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain" [DGKR18]
Location	Tel Aviv, Israel
Date	29 April- 3 May 2018
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	One of the flagship conferences of the the International Association for Cryptologic Research (IACR)
People reached	370 Research & scientific community

Title of conference	IEEE Symposium on Security and Privacy (SP) 2018
Type	Conference presentation and publication
Title of publication	"Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two" [DMMK18]
Location	San Francisco, USA
Date	May 21-23, 2018
Partners involved	UCL
People involved	Sebastian Meiser
Relevance to the project	Discussing the trade-off between anonymity, latency and bandwidth in anonymous communication networks. It showed that Loopix (the mix-net design on which PANORAMIX mix-net is based) is the best possible solution if we want to have a good anonymity, low latency and low bandwidth overhead. Since Oakland had only one track all the people present during the conference came to the talk, including both academics and industrial attendees. Also, the video of the presentation is available only, and so far more than 150 people saw it, which means this presentation can reach even a wider audience.
People reached	150 Research & scientific community

Title of conference	Data Justice 2018
Type	Conference participation/session chair
Location	Cardiff, UK
Date	May 21-22, 2018
Partners involved	UCL
People involved	George Danezis
Relevance to the project	Data Justice is the premier event in the UK on issues around data sovereignty, privacy and control. As such it complements our dissemination efforts to technical audiences, towards this other side of academia. Partly due to my role in PANORAMIX I was attending to take part in the advisory board of the Data Justice Lab project at Cardiff university, to which I am a member.
People reached	The audience was 150-200 researchers largely in the field of social sciences, arts and humanities.

Title of conference	SIGIR 2018
Type	Conference presentation and publication
Title of publication	"SynTF: Synthetic and Differentially Private Term Frequency Vectors for Privacy-Preserving Text Mining" [WK18]
Location	Ann Arbor, MI, USA
Date	July 8-12, 2018
Partners involved	SAP
People involved	Benjamin Weggenmann
Relevance to the project	Our PANORAMIX paper "SynTF: Synthetic and Differentially Private Term Frequency Vectors for Privacy-Preserving Text Mining" was accepted at SIGIR'18. The paper is joint work between Benjamin Weggenmann (SAP) and Florian Kerschbaum (University of Waterloo), and will be presented at the conference between July 8-12, 2018.
People reached	Audience at the academic conference included around 500 people.

Title of conference	Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)
Type	Conference presentation and publication
Title of publication	"POTs: The revolution will not be optimized?" [GOB18]
Location	Barcelona, Spain
Date	July 27, 2018
Partners involved	KUL, CCT
People involved	Rebekah Overdorf, David Stainton
Relevance to the project	We presented the paper on Protective Optimization Technologies, which proposes a new way to analyze the privacy impact of Big Data technologies in the environment, as well as how to design systems to protect us against them. This is relevant to the statistics use case of PANORAMIX, as the framework can be used to analyze its impact once deployed. CCT presented the messaging use-case work.
People reached	100 people from academia.

Title of conference	Symposium on Applications of Contextual Integrity (PrivaCI)
Type	Conference presentation and publication
Title of publication	"Position paper: On engineering AI agents for privacy"
Location	Princeton, USA
Date	13- 14 September 2018
Partners involved	KUL
People involved	Rafael Galvez
Relevance to the project	We presented a paper on engineering AI agents for privacy. It is specially relevant to WP6, as its engineers may also breach the privacy of their users by virtue of how they engineer the system.
People reached	90 people from academia.

Title of conference	11th Conference on Security and Cryptography for Networks (SCN)
Type	Conference presentation and publication
Title of publication	"On the Security Properties of e-Voting Bulletin Boards" [KKL+18]
Location	Amalfi, Italy
Date	September 5-7, 2018
Partners involved	UEDIN, UT
People involved	Aggelos Kiayias, Thomas Zacharias, Helger Lipmaa, Annabell Kuldmaa, Janno Siim
Relevance to the project	The presented paper analyses security properties of the most known bulletin board of Culnane and Schneider and points out its weaknesses. The paper is highly relevant to the project since bulletin boards are widely used in e-voting.
People reached	70 people mostly from academia.

Title of conference	Advances in Cryptology - 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018)
Type	Conference presentation and publication
Title of publication	"A Universally Composable Framework for the Privacy of Email Ecosystems" [CFKZ18]
Location	Brisbane, Australia
Date	December 2 – 6, 2018
Partners involved	UoA, UEDIN
People involved	Pyrros Chaidos, Olga Fourtounelli Aggelos Kiayias Thomas Zacharias
Relevance to the project	Asiacrypt is one of the most important cryptographic conferences gathering researchers from around the world. Presentation of the paper to the cryptography community.
People reached	200 people mostly from academia

3.3 Research Journal

Type	Journal publication
Title	"A Survey on Routing in Anonymous Communication Protocols"
Authors	Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Diaz [SSA+18]
Journal	ACM Computing Surveys (CSUR)
Date	May 2018
Partners involved	KUL
People involved	Claudia Diaz

Type	Journal publication
Title	"Towards Inferring Communication Patterns in Online Social Networks" [BPD17]
Authors	Ero Balsa, Cristina Pérez-Solà, and Claudia Diaz
Journal	ACM Transactions on Internet Technology 17(3)
Date	July 2017
Partners involved	KUL
People involved	Claudia Diaz

Type	Journal publication
Title	"The influence of differential privacy on short term electric load forecasting"
Authors	Günther Eibl, Kaibin Bao, Philip-William Grassal, Daniel Bernau, Hartmut Schmeck [EBG+18]
Journal	Energy Informatics 2018 1 (Suppl 1):48
Date	10 October 2018
Partners involved	SAP
People involved	Daniel Bernau

3.4 Policy Conference

Title of conference	PANORAMIX at Congreso de Privacidad (CDP) in Madrid 17-19 October
Type	Demo
Location	Madrid, Spain
Date	October 18, 2017
Partners involved	GRNET, Greenhost, KUL
People involved	Dimitris Mitroupoulos, Georgios Tsoukalas, Giorgos Korfiatis, Kali Kaneko, Meskio and Rafael Galvez
Relevance to the project	PANORAMIX took part in the H2020 joint dissemination activity at the European Privacy and Data Protection Summit co-organised by H2020 TYPES project, one of the other EU projects on privacy innovation.
People reached	300 experts in academia, government and industry.

Title of conference	7th International Conference on eDemocracy 2018
Type	Conference presentation and publication
Title of presentations	1) Communication privacy on the internet: the current status and technical challenges (Thomas Zacharias) 2) New directions in anonymity: the goals of the PANORAMIX project (Pyrros Chaidos) 3) The case of e-voting: a fully anonymous e-voting system(Panos Louridas)
Location	Athens, Greece
Date	December 15, 2017
Partners involved	UoA, UEDIN, GRNET
People involved	Pyrros Chaidos, Thomas Zacharias, Panos Louridas
Relevance to the project	Presenting the PANORAMIX project and goals to stakeholders and policy makers.
People reached	60 policy makers.

Title of conference	CPDP Panel 2018
Presentation Title	Anonymous Communications Infrastructures for the Protection of Metadata
Location	Brussels, Belgium
Date	January 24, 2018
Partners involved	KUL, UEDIN
People involved	Claudia Diaz, Aggelos Kiayias
Relevance to the project	PANORAMIX hosted a panel discussing the core of PANORAMIX.
Resources spent	€1200 panel cost and €2200 for panel members
People reached	1000 participants -diverse audience comprising scientific community, civil society, general public and policy makers,

Title of event	H2020 Project Clustering Workshop
Type	Presentation
Location	Athens, Greece
Date published	January 31, 2018
Partners involved	GRNET
People involved	Panos Louridas
Relevance to the project	Give more visibility to PANORAMIX at a workshop with 25 other H2020 projects. Video on ReCRED website

Title of event	"Stop worrying, trust the machine!? - Ethics and algorithms in a big data context"
Location	Leuven, Belgium
Date	March 22nd, 2018
Partners involved	KUL
People involved	Rafael Gálvez, Rebekah Overdorf, Marc Juarez
Relevance to the project	The conference explored the ethical and legal challenges with regards to Machine Learning and Big Data processes. This is relevant for one of statistics use case, as the use of AI algorithms and compliance with GDPR is a complex issue tackled in this symposium.
People reached	30 experts from academia and industry.

Title of event	Symposium: "The Role of Artificial Intelligence in Tomorrow's Society – Legal & Ethical Considerations"
Location	Leuven, Belgium
Date	March 26th, 2018
Partners involved	KUL
People involved	Rafael Gálvez
Relevance to the project	The symposium explored the ethical and legal considerations with regards to Artificial Intelligence and Machine Learning systems. This is relevant for one of statistics use case, as the use of AI algorithms and compliance with GDPR is a complex issue tackled in this symposium.
People reached	100 experts from academia and government.

Title of event	Cyberwatching.eu concertation meeting
Location	Brussels, Belgium
Date	April 26th, 2018
Partners involved	KUL
People involved	Claudia Diaz
Relevance to the project	PANORAMIX was presented as a relevant project for the European watch on cybersecurity & privacy.
People reached	70 experts from academia and government.

Title of event	ICT 2018 Imagine Digital - Connect Europe
Presentation Title	PANORAMIX: Privacy and Accountability in Networks via Optimized Randomized Mix-nets
Location	Vienna, Austria
Date	December 4-6, 2018
Partners involved	CCT, SAP, GRNET
People involved	Moritz Bartl, Benjamin Weggenmann, Dimitris Mitropoulos, Giorgos Korfiatis
Relevance to the project	Major dissemination event where all three use cases were presented to a large European audience.
People reached	1000 participants -diverse audience comprising people from industry, research and public bodies

Title of conference	CPDP Panel 2019
Presentation Title	"Anonymity loves company, and funding"
Location	Brussels, Belgium
Date	January 31, 2019
Partners involved	KUL, UEDIN, Greenhost, CCT
People involved	Claudia Diaz, Aggelos Kiayias, Harry Halpin, Moritz Bartl
Relevance to the project	PANORAMIX hosted a final dissemination panel discussing how to build anonymity systems that are successful in terms of attracting and sustaining a user-base, a development community, and the necessary funding to develop and run the systems.
Resources spent	€1200 panel cost and €3000 for panel members
People reached	1000 participants - diverse audience comprising scientific community, civil society, general public and policy makers

3.5 Industry Event

Industry events are particularly important to share PANORAMIX awareness among industry and government representatives. During such meetings the academic community has a great opportunity to show its research and explain why it matters to representatives beyond the scientific community. They also are great opportunity for researcher teams to find potential industry partners.

Event	Tor Developer's Conference
Location	Montreal, Canada
Date	October 11-16, 2017
Partners involved	CCT
People involved	David Stainton
Relevance to Project	Discussions with implementors of anonymity technologies, presentation of PANORAMIX.
People reached	50 from academia and industry

Event	London Enterprise Tech Meetup
Title of presentation	A witch-hunt for trojans in our chips
Location	London, UK
Date	February 12, 2018
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	Presentation on the problem of fabrication-time attacks and high-level overview of our solution based on multiparty computations.
People reached	50 from both government offices and the industry.

Activity	SAP Security Summit
Location	St. Leon-Rot, Germany
Date	February 13–14, 2018
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	We had our own booth on both days with a demo and poster presentation. We discussed PANORAMIX anonymization technologies with attendees of the event.
People reached	60 from Industry

Event	Tor Developer's Conference
Location	Rome, Italy
Date	March 11–15, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Discussions with implementors of anonymity technologies, presentation of PANORAMIX.
People reached	50 from academia and industry

Title of conference	RSA Conference 2018
Title of presentation	The Good, the Bad and the Ugly of the Ultrasonic Communications Ecosystem
Location	San Fransisco, US
Date	April 17, 2018
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	A formal introduction to a new communication channel based on ultrasounds, and the security and privacy challenges that come with it.
People reached	100 from academia, government and industry.

Activity	SAP Security Research Seminar
Location	Walldorf, Germany
Date	May 15, 2018
Partners involved	SAP
People involved	Benjamin Weggenmann
Relevance to the project	We presented and discussed our work on data anonymization in PANORAMIX with invited academic visitors and SAP employees. Data anonymization was one of four exclusive topics that had their own time slot.
People reached	20 Academic and Industry

Event	IMEC Technology Forum (ITF)
Location	Antwerp, Belgium
Date	May 23–24, 2018
Partners involved	UCL
People involved	George Danezis
Relevance to the project	ITF is an event organized by IMEC in Belgium, the Flemish engineering innovation body. I am presenting there our work on privacy and block chains, something that relates to our future exploitation strategy for PANORAMIX.
People reached	It gathers 200 participants which are a mix of industry and academia, as well as representatives from innovation branches of the Flemish government.

Event	Albania OpenLabs Technology Meetup
Title of presentation	Modern Mix Network Design
Location	Tirana, Albania
Date	July 6, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	The OpenLabs technology space in Tirana hosts open events for the technology community of Albania.
People reached	20 from Tech industry

Title of conference	Bitcoin Meetup
Title of presentation	Modern Mix Network Design
Location	Amsterdam, Netherlands
Date	August 1, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Presentation of PANORAMIX.
People reached	50 from Tech industry

Title of conference	Bornhack 2018
Title of presentation	Modern Mix Network Design
Location	Bornholm, Denmark
Date	August 8, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Presentation of mix networks to a diverse audience of hackers, makers, politicians, activists, developers, artists, sysadmins, and engineers.
People reached	50 from Tech industry

Title of conference	Zero Knowledge Summit
Title of presentation	Traffic analysis resistance with Mix Networks
Location	Berlin, Germany
Date	September 5, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Presentation of PANORAMIX.
People reached	100 from academia and industry

Activity	Tor Developer's Conference
Location	Mexico City, Mexico
Date	September 29 – October 3, 2018
Partners involved	CCT
People involved	David Stainton, Moritz Bartl
Relevance to the project	Discussions with implementers of anonymity technologies, presentation of PANORAMIX.
People reached	50 from academia and industry

3.6 Media Event

Title	The Loopix Anonymity System Wants to Be a More Secure Alternative to Tor
Location	https://www.bleepingcomputer.com/news/technology/the-loopix-anonymity-system-wants-to-be-a-more-secure-alternative-to-tor/
Date	September 16, 2017
Partners involved	UCL
People involved	Ania Piotrowska
Relevance to the project	Piece on Loopix.
People reached	Bleeping Computer has 700,000 members

Title	The Loopix Anonymity System Can Be A Good Tor Alternative, Comparison Shows
Location	https://fossbytes.com/loopix-anonymity-system-tor-alternative/
Date	September 18, 2017
Partners involved	UCL
People involved	Ania Piotrowska
Relevance to the project	Piece on Loopix.
People reached	Fossbytes has 5 million page views per month.

Title	Loopix: New Anonymization Service?
Location	https://www.deepdotweb.com/2017/10/02/loopix-new-anonymization-service//
Date	October 2, 2017
Partners involved	UCL
People involved	Ania Piotrowska
Relevance to the project	Piece on Loopix.
People reached	Deep.Dot.Web views per month not available.

Title	Loopix: A New Anonymity Network
Location	https://darkwebnews.com/anonymity/loopix/
Date	February 12, 2018
Partners involved	UCL
People involved	Ania Piotrowska
Relevance to the project	Piece on Loopix.
People reached	Dark Web News views per month not available.

Title	Are mixnets the answer to anonymous communications?
Location	https://www.csoonline.com/article/3304586/encryption/are-mixnets-the-answer-to-anonymous-communications.html
Date	September 11, 2018
Partners involved	UCL, UEDIN, Greenhost, CCT
People involved	Ania Piotrowska, Aggelos Kiayias, Harry Halpin, Moritz Bartl
Relevance to the project	Interview explaining the relevance of PANORAMIX and anonymization of metadata to a large security audience.
People reached	CSO has 786,000 average page views per month

Title	This Binance Labs-Backed Crypto Startup Wants to Anonymize Everything
Location	https://www.coindesk.com/this-binance-backed-crypto-startup-wants-to-anonymize-everything
Date	December 14, 2018
Partners involved	Greenhost, CCT, UCL
People involved	Harry Halpin, David Stainton, George Danezis
Relevance to the project	Article on Nym.
People reached	Coindesk has 22,000,000+ page views per month

3.7 Academic Workshops/Meetings

Workshop/Meeting	Meeting with the Chair for Information Security at the University of Stuttgart.
Location	Stuttgart, Germany
Date	September 26, 2017
Partners involved	SAP
People involved	Daniel Bernau
Relevance to the project	Topics included local differential privacy, as envisioned by PANORAMIX, and differential privacy in machine learning to gather future input for direction of these topics within PANORAMIX.
People reached	15 experts from academia.

Workshop/Meeting	Meeting with the Chair for Information Security at the University of Stuttgart.
Location	Stuttgart, Germany
Date	December 19, 2017
Partners involved	SAP
People involved	Benjamin Weggenmann
Relevance to the project	Discussions of re-identification attacks and possible countermeasures that are developed in PANORAMIX.

Workshop/Meeting	Real World Crypto Symposium
Location	Zürich, Switzerland
Date	January 10-12, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Connecting to academia and industry.

Workshop/Meeting	Round table on electronic voting for participatory budgeting
Location	Edinburgh, UK
Date	June 12, 2018
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	The purpose of this workshop was to bring together people from different areas and positions (Scottish government, academia, industry, and non-profit organisations) who share a common interest in e-voting, to participate in a round table discussion on the prospect of using e-voting and blockchain technologies for participatory budgeting (PB) – and other use cases – in Scotland.

Workshop/Meeting	Summer School on Real-world crypto and privacy
Location	Sibenic, Croatia
Date	June 11–15, 2018
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Connecting to academia and industry.

Workshop/Meeting	1st meeting of the IET Working Group on Electronic Voting
Location	IET Offices
Date	December 5, 2018
Partners involved	UEDIN
People involved	Thomas Zacharias
Relevance to the project	The initial focus of the group will be on the question of Internet Voting in the UK, and the aim is for the group to develop an informed and evidence-based position for the IET on this issue. The aim is for the work to inform policy discussions, and to feed into public debate.

3.8 Presentations

Venue/Community	ZISC Seminar ETH
Presentation Title	Towards Trojan-tolerant Cryptographic Hardware
Location	Zurich, Switzerland
Date	September 20, 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
People reached	30 systems and network security experts from academia.

Venue/Community	IMDEA Software Institute Seminar
Presentation Title	Cryptographic Hardware from Untrusted Components
Location	Madrid, Spain
Date	September 28, 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
People reached	30 security experts from academia and industry.

Venue/Community	Cryptacus Workshop
Presentation Title	Cryptographic Hardware from Untrusted Components
Location	Nijmegen, Netherlands
Date	November 16–18, 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
People reached	50 cryptography experts from academia and industry.

Venue/Community	Lecture at 34th Annual Chaos Communication Congress.
Presentation Title	Practical Mix Network Design
Location	Leipzig, Germany
Date	December 27–30, 2017
Partners involved	CCT
People involved	David Stainton
People reached	100 people from academia and industry at the live talk, several conversations with cryptography experts. Publication of video online.

Venue/Community	Lecture at Privacy For Everyone Conference.
Presentation Title	Anonymizing Cryptocurrencies From Network Observers With Mix Networks
Location	Berlin, Germany
Date	January 3, 2018
Partners involved	CCT
People involved	David Stainton
People reached	50 people from industry at the live talk. Publication of video online.

Venue/Community	Athecrypt 2018
Presentation Title	Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge
Location	Athens, Greece
Date	January 9, 2018
Partners involved	UoA
People involved	Pyrros Chaidos
People reached	50 research and scientific community

Venue/Community	Invited lecture at the Course on Secure Application Development (SecAppDev)
Presentation Title	Introduction to privacy technologies
Location	Leuven, Belgium
Date	February 19–23, 2018
Partners involved	KUL
People involved	Claudia Diaz
People reached	50 people mainly from industry.

Venue/Community	Chalmers Initiative Seminar
Presentation Title	The challenge of being anonymous on the Internet
Location	Gothenburg, Sweden
Date	March 15, 2018
Partners involved	KUL
People involved	Claudia Diaz
People reached	100 people from academia and industry.

Venue/Community	Stanford Security Seminar
Presentation Title	High-Assurance Cryptographic Hardware from Untrusted Components.
Location	Palo Alto, US
Date	April 19, 2018
Partners involved	UCL
People involved	Vasilios Mavroudis
People reached	30 security experts from academia.

Venue/Community	IInvited Lecture at the Summer School: Number theory and coding theory: Contemporary applications in security
Presentation Title	"ZK-SNARKs: foundations and applications"
Location	Turku, Finland
Date	May 28 –June 1, 2018
Partners involved	UT
People involved	Helger Lipmaa
People reached	50 people from academia

Venue/Community	Google Deepmind London
Presentation Title	"Using mix-networks for building anonymous communication systems"
Location	London, UK
Date	August 1, 2018
Partners involved	UCL
People involved	Ania Piotrowska
People reached	Internal Google seminar, 25 people

Venue/Community	Presentation at the Information Systems and Security Lab Seminar, Sharif University of Technology
Presentation Title	"A Subversion-Resistant SNARK"
Location	Tehran, Iran
Date	August 1, 2018
Partners involved	UT
People involved	Karim Baghery
People reached	25 people from academia

Venue/Community	Keynote talk at PET-CON
Presentation Title	Mixnets and Recent Advancements in the PANORAMIX Project
Location	Hamburg, Germany
Date	October 11–12 , 2018
Partners involved	KUL
People involved	Claudia Diaz
People reached	30 people from academia.

Venue/Community	Seminar presentation at the Joint Estonian-Latvian Theory Days 2018
Presentation Title	"On the Security Properties of e-Voting Bulletin Boards"
Location	Riga, Latvia
Date	October 12–14, 2018,
Partners involved	UT
People involved	Helger Lipmaa, Janno Siim
People reached	25 people from academia

3.9 Cross PANORAMIX visits

Activity	WP4/WP7 Integration Sprint
Location	Athens
Date	December 2017
Partners involved	CCT, Greenhost, GRNET
People involved	Moritz Bartl, David Stainton, Vincent Breitmoser, Meskio, Kali, Georgios Tsoukalas, Giorgos Korfiatis, Panos Louridas
Relevance to the project	Integration of WP4 and WP7

Activity	PANORAMIX Project Steering Committee face to face meeting
Location	BLOOM hotel Brussels
Date	January 23, 2018
Partners involved	UEDIN, UCL, UT, UoA, KUL, GH, SAP, GRNET, CCT, External Advisory Board (EAB) and guests
People involved	Aggelos Kiayias, Thomas Zacharias, Mirjam Wester (UEDIN), George Danezis, Vasilios Mavroudis (UCL), Michał Zając, Janno Siim (UT), Pyrros Chaidos (UoA), Claudia Diaz, Rafael Galvez, Rebekah Ostendorf(KUL), Harry Halpin, Sacha van Geffen (GH), Benjamin Weggenmann (SAP), Panos Louridas (GRNET), Moritz Bartl (CCT) Gus Hosein, Marit Hansen (External Advisory Board), Merel Koning, Carmela Trancoso, Zaki Mannian & Privacy Camp attendees
Relevance to the project	Full day meeting presenting the progress in PANORAMIX to the consortium, the EAB and other interested parties.
Resources spent	1 PM and €2100 (meeting facilities & catering)
People reached	Internal PANORAMIX dissemination - 23 people

Activity	PANORAMIX Project Steering Committee face to face meeting
Location	Athens
Date	September 24, 2018
Partners involved	UEDIN, UCL, UT, UoA, KUL, GH, SAP, GRNET, CCT, External Advisory Board (EAB) and guests
People involved	Aggelos Kiayias, Thomas Zacharias, Mirjam Wester (UEDIN), Ania Piotrowska (UCL), Michał Zając, Janno Siim (UT), Pyrros Chaidos (UoA), Claudia Diaz, Rafael Galvez, Rebekah Ostendorf. Elena Andreeva (KUL), Harry Halpin, Sacha van Geffen (GH), Benjamin Weggenmann (SAP), Panos Louridas,Giorgos Korfiatis, Georgios Tsoukalas, Dimitris Mitroupolis (GRNET),David Stainton, Moritz Bartl (CCT) Sven Heiberg, Bart Preneel (External Advisory Board), Merel Koning + external guests
Relevance to the project	Full day meeting presenting the progress in PANORAMIX to the consortium, the EAB and other interested parties.
People reached	Internal PANORAMIX dissemination - 30 people

Activity	Transfer of knowledge WP3 - WP5
Location	Athens, Greece
Date	September 24-28, 2018
Partners involved	UT, GRNET
People involved	Panos Louridas, Janno Siim, Michał Zając
Relevance to the project	Transfer of knowledge WP3 - WP5

3.10 Training Courses, Videos and Documentation

Type	Demo of our secure infrastructure
Location/URL	https://github.com/OpenCryptoProject/JCMathLib
Date published	October 18, 2017
Partners involved	UCL
People involved	Vasilios Mavroudis, Petr Svenda
Project Description	Open source cryptographic library for smartcards. It is the first library of its kind to ever become public.

Activity	Interdisciplinary Summer School on Privacy (ISP)
Location	Nijmegen, the Netherlands
Type	co-Organiser and participation in summer school
Date	9-13 July 2018
Partners involved	KUL
People involved	Claudia Diaz, Rafael Galvez
Project Description	The interdisciplinary summerschool on privacy provides an intensive one week academic post-graduate programme teaching privacy from a technical, legal and social perspective. The theme "AI, Algorithms & Privacy" addresses the privacy issues that arise from the use of Artificial Intelligence and machine learning algorithms, and studies how to address these issues. It was highly relevant for the statistics use case of PANORAMIX, providing new ways of looking at the interaction of the Machine Learning application, the PANORAMIX anonymization framework and the final user.

3.11 Repositories

Type	Git Repository
Location/URL	https://github.com/grnet/panoramix
Partners involved	GRNET
People involved	Giorgos Korfiatis, Georgios Tsoukalas
Project Description	PANORAMIX mixnet server and client.

Type	Git Repository
Location/URL	https://github.com/UCL-InfoSec/sphinx
Partners involved	UCL
People involved	Ania Piotrowska, George Danezis
Project Description	Implementation of the Sphinx mix packet format core cryptographic functions.

Type	Git Repository
Location/URL	https://github.com/UCL-InfoSec/loopix
Partners involved	UCL
People involved	Ania Piotrowska, George Danezis
Project Description	The public repository of the Loopix mix system.

Type	Git Repository
Location/URL	https://github.com/druid/mcmix-benchmark
Partners involved	UEDIN
People involved	Thomas Zacharias
Project Description	MCMix Code

Type	Git Repositories
Location/URL	https://github.com/Katzenpost/
Partners involved	CCT, Greenhost, KUL
People involved	Moritz Bartl, Claudia Diaz, Kali Kaneko, Ania Piotrowska, David Stainton, Yawning Angel
Project Description	PANORAMIX E-Mail Decryption Mix net, source code and documentation

Type	Git Repository
Location/URL	https://github.com/OpenCryptoProject/JCMathLib
Date published	October 18, 2017
People involved	Vasilios Mavroudis, Petr Svenda
Project Description	Open source cryptographic library for smartcards. It is the first library of its kind to ever become public.

Type	Git Repository
Location/URL	https://github.com/OpenCryptoProject/Myst
Partners involved	UCL
People involved	Vasilios Mavroudis, Petr Svenda
Project Description	The source code of our secure mix-net infrastructure prototype.

Type	Git Repository
Location/URL	https://github.com/ubeacsec/Silverdog
Partners involved	UCL
People involved	Vasilios Mavroudis
Project Description	Browser extension preventing unauthorized tracking with ultrasounds. [MHF+17]

4. Progress monitoring

The key performance indicators (KPI), with yearly targets, and the total actual activity for all partners are found in Table 4.1. Overall targets have been met with some even substantially surpassed. Especially the large number of publications at research conferences and in research journals are again a testament to the outstanding research that is being carried out in PANORAMIX as all these are peer-reviewed publications.

In addition to the two categories introduced in D2.9, "Presentations" and "Cross PANORAMIX visits" which in this final year tallied 13 for Presentations and 4 for Cross site visits we included the list of git repositories which are an important legacy item for PANORAMIX.

Dissemination Type	Actual	Target (per year)
User-facing website articles and blog posts	12	12
Industry Event	12	6
Policy Conference	8	3
Media Event	6	2
Research Conference Publications	17	6
Research Journal Publications	3	3
Training Courses, Videos & Documentation	2	3

Table 4.1: Dissemination Key Performance Indicators

Bibliography

[ABLZ17] Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michal Zajac. A subversion-resistant SNARK. In *ASIACRYPT (3)*, volume 10626 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2017.

[BPD17] Ero Balsa, Cristina Pérez-Solà, and Claudia Díaz. Towards inferring communication patterns in online social networks. *ACM Trans. Internet Techn.*, 17(3):32:1–32:21, 2017.

[CFKZ18] Pyrros Chaidos, Olga Fourtounelli, Aggelos Kiayias, and Thomas Zacharias. A universally composable framework for the privacy of email ecosystems. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, pages 191–221, 2018.

[DGKR18] Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *EUROCRYPT (2)*, volume 10821 of *Lecture Notes in Computer Science*, pages 66–98. Springer, 2018.

[DMMK18] Debajyoti Das, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Anonymity trilemma: Strong anonymity, low bandwidth overhead, low latency - choose two. In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*, pages 108–126, 2018.

[EBG+18] Günther Eibl, Kaibin Bao, Philip-William Grassal, Daniel Bernau, and Hartmut Schmeck. The influence of differential privacy on short term electric load forecasting. *CoRR*, abs/1807.02361, 2018.

[FLSZ17] Prastudy Fauzi, Helger Lipmaa, Janno Siim, and Michal Zajac. An efficient pairing-based shuffle argument. In *ASIACRYPT (2)*, volume 10625 of *Lecture Notes in Computer Science*, pages 97–127. Springer, 2017.

[GG18] Rafa Galvez and Seda Gurses. The odyssey: Modeling privacy threats in a brave new world. In *2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2018, London, United Kingdom, April 23-27, 2018*, pages 87–94, 2018.

[GKLP18] Juan A. Garay, Aggelos Kiayias, Nikos Leonardos, and Giorgos Panagiotakos. Bootstrapping the blockchain, with applications to consensus and fast PKI setup. In *Public Key Cryptography (2)*, volume 10770 of *Lecture Notes in Computer Science*, pages 465–495. Springer, 2018.

[GOB18] Seda Gurses, Rebekah Overdorf, and Ero Balsa. Pots: The revolution will not be optimized? *CoRR*, abs/1806.02711, 2018.

[JJG+18] Rob Jansen, Marc Juárez, Rafa Galvez, Tariq Elahi, and Claudia Díaz. Inside job: Applying traffic analysis to measure tor from within. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*, 2018.

[KKL+18] Aggelos Kiayias, Annabell Kuldmaa, Helger Lipmaa, Janno Siim, and Thomas Zacharias. On the security properties of e-voting bulletin boards. In *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, pages 505–523, 2018.

[MCS+17] Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec, and George Danezis. A touch of evil: High-assurance cryptographic hardware from untrusted components. In *CCS*, pages 1583–1600. ACM, 2017.

[MHF+17] Vasilios Mavroudis, Shuang Hao, Yanick Fratantonio, Federico Maggi, Christopher Kruegel, and Giovanni Vigna. On the privacy and security of the ultrasound ecosystem. *Proceedings on Privacy Enhancing Technologies*, 2017(2):95–112, 2017.

[MV18] Vasilios Mavroudis and Michael Veale. Eavesdropping whilst you're shopping: Balancing personalisation and privacy in connected retail spaces. 2018.

[OJA+17] Rebekah Overdorf, Mark Juárez, Gunes Acar, Rachel Greenstadt, and Claudia Díaz. How unique is your .onion?: An analysis of the fingerprintability of tor onion services. In *CCS*, pages 2021–2036. ACM, 2017.

[PHG+17] Ania M. Piotrowska, Jamie Hayes, Nethanel Gelernter, George Danezis, and Amir Herzberg. Annotify: A private notification service. In *WPES@CCS*, pages 5–15. ACM, 2017.

[RPJ+18] Vera Rimmer, Davy Preuveneers, Marc Juárez, Tom van Goethem, and Wouter Joosen. Automated website fingerprinting through deep learning. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*, 2018.

[SSA+18] Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Díaz. A survey on routing in anonymous communication protocols. *ACM Comput. Surv.*, 51(3):51:1–51:39, 2018.

[TDE17] Raphael R. Toledo, George Danezis, and Isao Echizen. Mix-oram: Using delegated shuffles. In *WPES@CCS*, pages 51–61. ACM, 2017.

[WK18] Benjamin Weggenmann and Florian Kerschbaum. Syntf: Synthetic and differentially private term frequency vectors for privacy-preserving text mining. In *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval, SIGIR 2018, Ann Arbor, MI, USA, July 08-12, 2018*, pages 305–314, 2018.