Mirjam Wester—Ed. (UEDIN)
Vasilios Mavroudis (UCL)
Harry Halpin (GH)
Michał Zając (UT)
Benjamin Weggenmann (SAP)
Rafael Galvez (KUL)
Aggelos Kiayias (UEDIN)

Dissemination Report II

Deliverable D2.9

August 31, 2017
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Revision History

Revision	Date	Author(s)	Description
0.1	2017-02-20	MW (UEDIN)	Initial draft
0.5	2017-08-04	MW(UEDIN)	Incorporated partners' dissemination activities
0.6	2017-08-13	RG (KUL)	Review
0.7	2017-08-17	MW (UEDIN)	Revision after review
0.8	2017-08-28	AK (UEDIN)	Final review
1.0	2017-08-31	MW(UEDIN)	Final version and submission to the EC
1.1	2017-09-25	MW(UEDIN)	Missing SAP activities included

Executive Summary

This dissemination report, the second of three, encompasses the dissemination activities of the project partners for the time period from September 2016 through to August 2017. Activities such as web-site, publications, conference visits and industry events are reported. In summary, all of the targeted dissemination channels were utilized with almost 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 second 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 2016 through to August 2017. 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 (D2.9) 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, D2.9 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]
- D2.10 - Dissemination Report III [UEDIN]

2. 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.

2.1 User-facing website articles, blog posts and twitter

Short descriptions of the blog posts published during Y2 are given in this section. The relevance of the blog posts to the project is mainly to ensure interested parties have a way of staying informed on the activities and events PANORAMIX is involved with. The resources spent on writing the blog posts vary between about 10-20 min (for most posts) to a slightly larger time investment but never more that 0.05 PM. A rough estimate of the number of people reached for the blog posts on panoramix-project.eu are indicated in Figure 2.1 which shows Google web analytics data for the PANORAMIX website. On average there are 200 sessions a month.

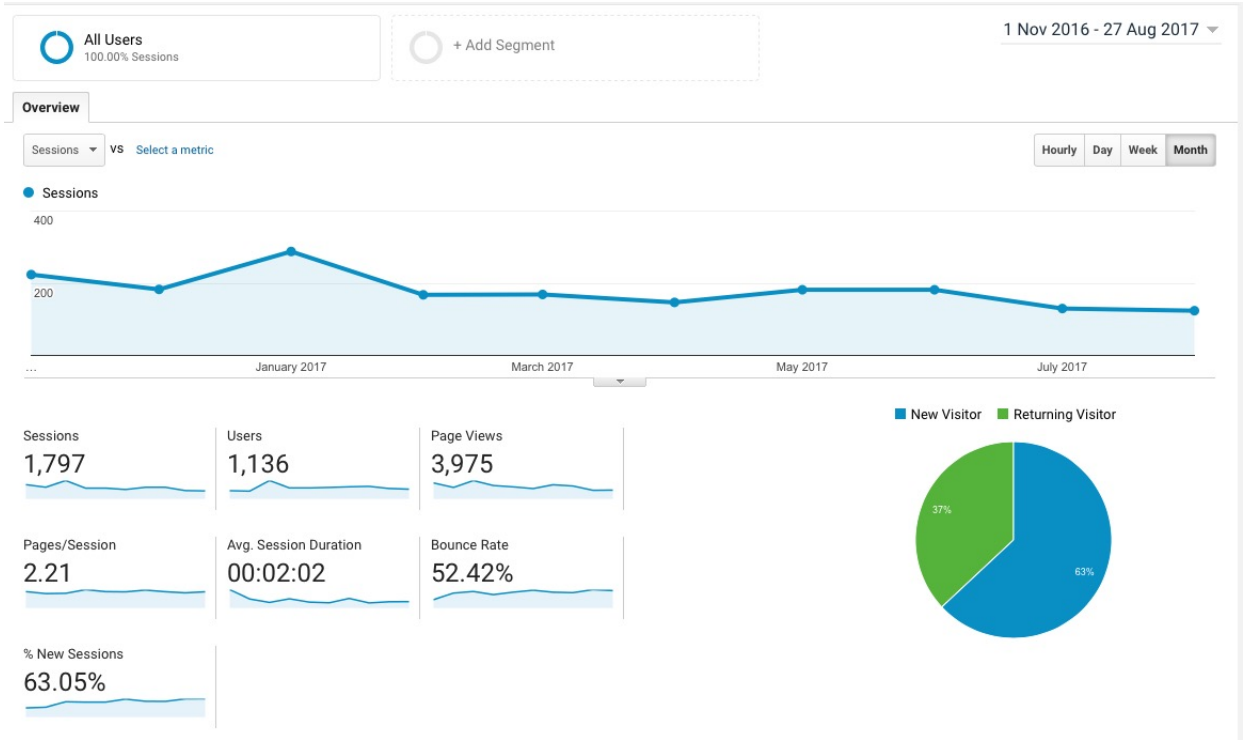

Figure 2.1: Analytics of the PANORAMIX website.

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 PANORAMIX stands at 94 (31/8/2017). Figure 2.1 shows the number of impressions that the tweets have attracted every month since October 2016, and the number of new followers each month. The peak in January coincides with PANORAMIX's participation in CPDP and the release of the PANORAMIX video.

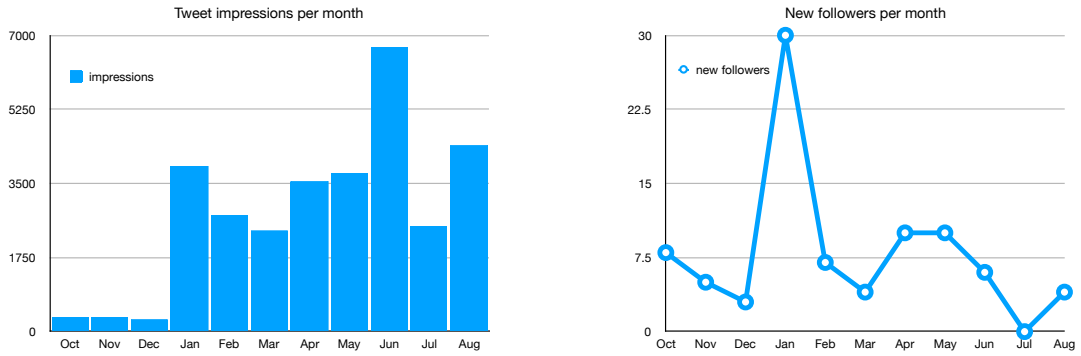

Figure 2.2: Analytics of the PANORAMIX twitter account.

The following blog posts have been published on the PANORAMIX website during Y2.

Title	New publication from PANORAMIX members to appear in ASIACRYPT 2016
Type	Blog post
Location/URL	https://panoramix-project.eu/new-publication-from-panoramix-team-members-to-appear-in-asiacrypt-2016/
Date published	13 September 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Advertising of a new PANORAMIX publication with links where to find it. Dissemination to the wider public.

Title	An ASIACRYPT paper on zero-knowledge shuffles
Type	Blog post
Location/URL	https://panoramix-project.eu/an-asiacrypt-paper-on-zero-knowledge-shuffles/
Date published	14 September 2016
Partners involved	UT
People involved	Helger Lipmaa, Michał Zając
Relevance to the project	Advertising of a new PANORAMIX publication with links where to find it. Dissemination to the wider public.

Title	Presentation about the science of the blockchain and privacy in Scottish Enterprise
Type	Blog post
Location/URL	https://panoramix-project.eu/presentation-about-the-science-of-the-blockchain-and-privacy-in-scottish-enterprise/
Date published	28 September 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Dissemination of the ongoing work of the Panoramix consortium to an audience which included many key IT industry actors in Scotland.

Title	PANORAMIX at ACM CCS (24-28 October 2016)
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-acm-ccs-24-28-october-2016/
Date published	27 October 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Attendance of an important conference in the field, with a short description and links to the two PANORAMIX-related papers presented at the conference.

Title	Presentation at the Alan Turing Institute
Type	Blog post
Location/URL	https://panoramix-project.eu/presentation-at-the-alan-turing-institute/
Date published	1 November 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Presentation of ongoing work of the PANORAMIX consortium and discussion what Blockchain technology might mean for UK institutions and what the research challenges for the Turing Institute are.

Title	PANORAMIX at Real World Cryptography conference 2017
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-at-real-world-cryptography-conference-2017/
Date published	30 January 2017
Partners involved	UEDIN
People involved	Agggelos Kiayias
Relevance to the project	Further dissemination of the involvement of PANORAMIX at a large international cryptography conference.

Title	PANORAMIX demo at CPDP
Type	Blog post
Location/URL	https://panoramix-project.eu/cpdp-demo/
Date published	2 February 2017
Partners involved	All consortium partners
People involved	All
Relevance to the project	PANORAMIX had a stall at the conference to present the PANORAMIX demo, the blog post describes this dissemination activity.

Title	Security seminar at Newcastle University
Type	Blog post
Location/URL	https://panoramix-project.eu/security-seminar-at-newcastle-university/
Date published	8 March 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	A presentation about "End-to-end verifiable elections" at the Newcastle School of Computing Science including PANORAMIX research.

Title	New publication to be presented in PKC 2017 conference
Type	Blog post
Location/URL	https://panoramix-project.eu/new-publication-to-be-presented-in-pkc-2017-conference/
Date published	9 March 2017
Partners involved	UEDIN
People involved	Thomas Zacharias, Aggelos Kiayias
Relevance to the project	Advertising of a new PANORAMIX publication with links where to find it. Dissemination to the wider public.

Title	SAP D-KOM 2017
Type	Blog post
Location/URL	https://panoramix-project.eu/sap-d-kom-2017/
Date published	13 March 2017
Partners involved	SAP
People involved	Benjamin Weggenmann
Relevance to the project	Dissemination by the PANORAMIX SAP team to others in the industry. The team introduced PANORAMIX to stakeholders within SAP by presenting and demonstrating the PANORAMIX research results on anonymization.

Title	PANORAMIX meets Tor: Work Package 7 f2f meeting March 27-28th Amsterdam
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-meets-tor-work-package-7-f2f-meeting-march-27-28th-amsterdam/
Date published	17 March 2017
Partners involved	GH, UCL, KUL, UEDIN
People involved	Anna Piotrowska, Claudia Diaz, Harry Halpin, Kali Kaneko, Moritz Bartl, Tariq Elahi, Thomas Zacharias
Relevance to the project	The blog post describes the WP7 meeting of PANORAMIX members with the long-standing Tor network.

Title	Smart contracts day – March 31st – Athens
Type	Blog post
Location/URL	https://panoramix-project.eu/smart-contracts-day-march-31st-athens/
Date published	22 March 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Interaction with a diverse group of people on the topic of Information, Privacy and Smart Contracts in the interdisciplinary field merging Cryptography and Law. PANORAMIX work was included in the presentation.

Title	New partner — CCT
Type	Blog post
Location/URL	https://panoramix-project.eu/new-partner-cct/
Date published	10 April 2017
Partners involved	CCT
People involved	Moritz Bartl, Vincent Breitmoser
Relevance to the project	Publishing news of a new partner in the consortium.

Title	The UCL Carnival of Decentralization and Privacy
Type	Blog post
Location/URL	https://panoramix-project.eu/the-ucl-carnival-of-decentralization-and-privacy/
Date published	12 June 2017
Partners involved	UCL, KUL, UEDIN
People involved	George Danezis, Claudia Diaz, Aggelos Kiayias
Relevance to the project	Report on the UCL Carnival co-sponsored by PANORAMIX.

Title	Panoramix presentations at 2017 Summer Schools
Type	Blog post
Location/URL	https://panoramix-project.eu/panoramix-presentations-at-2017-summer-schools/
Date published	26 June 2017
Partners involved	UCL and UEDIN
People involved	George Danezis (UCL), Aggelos Kiayias (UEDIN)
Relevance to the project	Blog post reporting on tutorials given at 2017 summer schools which included PANORAMIX research.

Title	MCMix anonymous messaging system to be presented in USENIX security conference
Type	Blog post
Location/URL	https://panoramix-project.eu/mcmix-anonymous-messaging-system-to-be-presented-in-usenix-security-conference/
Date published	12 August 2017
Partners involved	UEDIN
People involved	Thomas Zacharias, Aggelos Kiayias (UEDIN)
Relevance to the project	Blog post on PANORAMIX work at the prestigious USENIX conference.

2.2 Research Conference

This section lists the research conferences that PANORAMIX has been involved with during Y2. 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.

Title of conference	21st European Symposium on Research in Computer Security (ESORICS 2016)
Type	Conference presentation and publication
Title of publication	"Toward an Efficient Website Fingerprinting Defense" [JIP+16]
Location	Heraklion, Crete, Greece
Date	26-30 September 2016
Partners involved	KUL
People involved	Claudia Diaz
Relevance to the project	Good security conference, one of the main venues in Europe for cybersecurity.
Resources spent	0.05 PM
People reached	150 Research and scientific community

Title of conference	21st European Symposium on Research in Computer Security (ESORICS 2016)
Type	Conference presentation and publication
Title of publication	"Efficient Encrypted Keyword Search for Multi-user Data Sharing" [KOR+16]
Location	Heraklion, Crete, Greece
Date	26 -30 September 2016
Partners involved	UEDIN
People involved	Aggelos Kiayas
Relevance to the project	Good security conference, one of the main venues in Europe for cybersecurity.
Resources spent	0.05 PM
People reached	150 Research and scientific community

Title of conference	23rd ACM Conference on Computer and Communications Security (ACM CCS 2016)
Type	Conference presentation and publication
Title of publication	"SFADiff: Automated Evasion Attacks and Fingerprinting Using Black-box Differential Automata Learning" [ASJ+16]
Location	Vienna, Austria
Date	24-28 October 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Presenting PANORAMIX work at a top tier cybersecurity conference.
Resources spent	0.05 PM
People reached	800 Research and scientific community

Title of conference	23rd ACM Conference on Computer and Communications Security (ACM CCS 2016)
Type	Conference presentation and publication
Title of publication	"Practical Non-Malleable Codes from l-more Extractable Hash Functions" [KLT16]
Location	Vienna, Austria
Date	24-28 October 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Presenting PANORAMIX work at a top tier cybersecurity conference.
Resources spent	0.05 PM
People reached	800 Research and scientific community

Title of conference	Advances in Cryptology - 22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016)
Type	Conference presentation and publication
Title of publication	"Indistinguishable Proofs of Work or Knowledge" [BKZZ16]
Location	Hanoi, Vietnam
Date	4-8 December 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Presenting PANORAMIX research.
Resources spent	0.1 PM
People reached	250 Research and scientific community

Title of conference	Advances in Cryptology - 22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016)
Type	Conference presentation and publication
Title of publication	"A Shuffle Argument Secure in the Generic Model" [FLZ16]
Location	Hanoi, Vietnam
Date	4-8 December 2016
Partners involved	UT
People involved	Helger Lipmaa, Michał Zając
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.
Resources spent	0.1 PM
People reached	250 Research and scientific community

Title of conference	Real World Cryptography Conference 2017
Type	Conference organisation
Location	Columbia University in New York City
Date	4-6 January 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Aggelos Kiayias co-organised the conference and is further involved with RWC as a member of the Steering Committee. Aggelos also participated in the technical program of the conference with a contributed talk "Productizing TLS Attacks: The Rupture API" co-authored with Eva Sarafianou and Dionysis Zindros.
Resources spent	0.05 PM
People reached	600 Research and scientific community

Title of conference	20th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC 2017)
Type	Conference presentation and publication
Title of publication	"CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions" [BBL17]
Location	Amsterdam, The Netherlands
Date	28-31 March 2017
Partners involved	UT
People involved	Helger Lipmaa
Relevance to the project	Presentation of the paper to the cryptography community.
Resources spent	0.05 PM
People reached	120 Research and scientific community

Title of conference	20th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC 2017)
Type	Conference presentation and publication
Title of publication	"Ceremonies for End-to-End Verifiable Elections" [KZZ17b]
Location	Amsterdam, The Netherlands
Date	28-31 March 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Specialised cryptography conference.
Resources spent	0.1 PM
People reached	120 Research and scientific community

Title of conference	Financial Cryptography and Data Security 2017
Type	Conference presentation and publication
Title of publication	"Optimally Sound Sigma Protocols Under DCRA" [Lip17]
Location	Malta
Date	3-7 April 2017
Partners involved	UT
People involved	Helger Lipmaa
Relevance to the project	Presentation of the paper to the cryptography research community.
Resources spent	0.05 PM
People reached	200 Research and scientific community

Title of conference	Financial Cryptography and Data Security 2017
Type	Conference presentation and publication
Title of publication	"A Simpler Rate-Optimal CPIR Protocol" [LP17]
Location	Malta
Date	3-7 April 2017
Partners involved	UT
People involved	Helger Lipmaa
Relevance to the project	Presentation of the paper to the cryptography research community.
Resources spent	0.05 PM
People reached	200 Research and scientific community

Title of conference	Computability in Europe 2017
Type	Conference presentation
Location	Turku, Finland
Date	12-16 June 2017
Partners involved	UT
People involved	Helger Lipmaa
Relevance to the project	Presentation of the paper "A Shuffle Argument Secure in the Generic Model" [FLZ16] to computer scientists.
Resources spent	0.05 PM
People reached	120 Research and scientific community

Title of conference	Privacy Enhancing Technologies Symposium
Type	Conference presentation
Location	Minneapolis, MN, USA
Date	17-22 July 2017
Partners involved	CCT
People involved	David Stainton
Relevance to the project	Short presentation as part of the Rump Sessions about the WP7 work.
Resources spent	0.05 PM
People reached	50 Research and scientific community

Title of conference	31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'17)
Type	Conference presentation and publication
Title of publication	"Privacy-Preserving Outlier Detection for Data Streams" [BBK17]
Location	Philadelphia, PA, USA
Date	19–21 July 2017
Partners involved	SAP
People involved	Daniel Bernau
Relevance to the project	DBSec is an annual international conference covering research in data and applications security and privacy.
Resources spent	0.05 PM
People reached	30 Research and scientific community

Title of conference	26th USENIX Security Symposium (USENIX Security 17)
Type	Conference presentation and publication
Title of publication	"The Loopix Anonymity System" [PHE+17]
Location	Vancouver, BC, Canada
Date	16-18 August, 2017
Partners involved	UCL, KUL
People involved	Ania Piotrowska, Jamie Hayes, Sebastian Meiser, George Danezis (UCL), Tariq Elahi (KUL)
Relevance to the project	Top-tier conference world-wide. The place to get the word out about PANORAMIX findings.
Resources spent	0.4 PM
People reached	500 Research and scientific community

Title of conference	26th USENIX Security Symposium (USENIX Security 17)
Type	Conference presentation and publication
Title of publication	"MCMix: Anonymous Messaging via Secure Multiparty Computation" [AKTZ17]
Location	Vancouver, BC, Canada
Date	16-18 August, 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Top-tier conference world-wide. The place to get the word out about PANORAMIX findings.
Resources spent	0.1 PM
People reached	500 Research and scientific community

Title of conference	CRYPTO 2017
Type	Conference presentation and publication
Title of publication	"Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol." [KRDO17]
Location	Santa Barbara, CA, USA
Date	21 August 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	CRYPTO, the International Cryptology Conference, is one of the largest academic conferences in cryptography and cryptanalysis.
Resources spent	0.05 PM
People reached	500 Research and scientific community

Title of conference	CRYPTO 2017
Type	Conference presentation and publication
Title of publication	"The Bitcoin Backbone Protocol with Chains of Variable Difficulty" [GKL17]
Location	Santa Barbara, CA, USA
Date	21 August 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	CRYPTO, the International Cryptology Conference, is one of the largest academic conferences in cryptography and cryptanalysis.
Resources spent	0.05 PM
People reached	500 Research and scientific community

2.3 Research Journal

Type	Journal publication
Title	Auditing for privacy in threshold PKE e-voting [KZZ17a]
Authors	Aggelos Kiayias, Thomas Zacharias and Bingsheng Zhang
Journal	Information & Computer Security
Date	4 December 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Journal publications provide a valuable, and respected, resource for researchers to learn about PANORAMIX research.
Resources spent	0.5 PM writing the paper

Type	Journal publication
Title	On the Privacy and Security of the Ultrasound Ecosystem [MHF+17]
Authors	Vasilios Mavroudis, Shuang Hao, Yanick Fratantonio, Federico Maggi, Giovanni Vigna, and Christopher Kruegel
Journal	Proceedings on Privacy Enhancing Technologies (PoPETs)
Date	4 April 2017 (Published online)
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	Journal publications provide a valuable, and respected, resource for researchers to learn about PANORAMIX research.
Resources spent	0.5 PM writing the paper

Type	Journal publication
Title	Website Fingerprinting Defenses at the Application Layer [CHJ17]
Authors	Giovanni Cherubin, Jamie Hayes and Marc Juarez
Journal	Proceedings on Privacy Enhancing Technologies (PoPETs)
Date	4 April 2017 (Published online)
Partners involved	UCL, KUL
People involved	Jamie Hayes (UCL) Marc Juarez (KUL)
Relevance to the project	Journal publications provide a valuable, and respected, resource for researchers to learn about PANORAMIX research.
Resources spent	0.5 PM writing the paper

Type	Journal publication
Title	An Efficient E2E Verifiable E-voting System without Setup Assumptions [KZZ17c]
Authors	Aggelos Kiayias, Thomas Zacharias and Bingsheng Zhang
Journal	IEEE Security & Privacy
Date	29 June 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias, Thomas Zacharias
Relevance to the project	Journal publications provide a valuable, and respected, resource for researchers to learn about PANORAMIX research.
Resources spent	0.5 PM writing the paper

2.4 Policy Conference

Activity	CPDP Computers, Privacy & Data Protection: The age of intelligent machines
Type	Conference demo
Location	Brussels, Belgium
Date	25 & 26 January 2017
Partners involved	All consortium partners
People involved	Aggelos Kiayias, Thomas Zacharias, Mirjam Wester (UEDIN), George Danezis, Ania Piotrowska (UCL), Helger Lipmaa, Michał Zając, Annabell Kuldmaa (UT), Pyrros Chaidos (UoA), Claudia Diaz, Rafael Galvez, Tariq Elahi (KUL), Harry Halpin, Kali Kaneko, Mooness Davarian (GH/LEAP), Benjamin Weggenmann (SAP), Panos Louridas, Dimitris Mitropoulos, Geore Korfiatis, Giorgos Tsoukalas (GRNET), Moritz Bartl (CCT)
Relevance to the project	Panoramix had a booth at CPDP and presented the project on Thursday 26 January. GRNET and Greenhost/LEAP presented their respective demos a chat room demo and an e-mail demo. The Panoramix video was shown on a big screen on a loop.
Resources spent	1 PM and €675 (cost of hiring booth)
People reached	1000 participants (divers audience comprising: scientific community, civil society, general public and policy makers)

Activity	LEAP meeting
Location	Barcelona, Spain
Date	14-17 March 2017
Partners involved	GH
People involved	Harry Halpin, Michiel Nuyts, Kali Kaneko, Moo Davarian
Relevance to the project	Meeting with other open source coders working on same codebase, introducing them to PANORAMIX.
Resources spent	0.5 PM
People reached	12 other coders working on mix nets and email, including Jeff Burdges (Inria)

2.5 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.

Activity	Black Hat briefing "CTX: eliminating breach with context hiding"
Location	London, UK
Date	4 November 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Present and discuss results with the brightest professionals and researchers in the industry. Black Hat is the most technical and relevant global information security event series in the world.
Resources spent	0.05 PM
People reached	200 Industry

Activity	Black Hat briefing "Talking Behind Your Back: Attacks and Countermeasures of Ultrasonic Cross-Device Tracking"
Location	London, UK
Date	4 November 2016
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	The audience consisted of security professionals. We briefly presented the architecture of a modern anonymity network they were familiar with, introduced a series of attacks against such networks.
Resources spent	0.05 PM
People reached	200 Industry

Activity	Talk at Chaos Communication Congress "Talking Behind Your Back"
Location	Hamburg, Germany (also streamed)
Date	27-30 December 2016.
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	The audience was very heterogeneous, with a deep interest in technical aspects of anonymity networks and threats. For this reason, we presented the architecture of a modern anonymity network they were familiar with, and then built upon this knowledge to discuss privacy implications of modern threats against the network. One core element of the presentation was a novel class of attacks that we uncovered, and the audience was particularly enthusiastic on discussing potential extensions.
Resources spent	0.05 PM
People reached	500 General Public, Other

Activity	SAP® Development Kick-Off Meeting
Location	Karlsruhe, Germany
Date	11 & 12 January 2017
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	The German SAP development community came together on January 11 and 12 in Karlsruhe for the annual SAP® Development Kick-Off Meeting, the first and largest event of the series to be held in 14 SAP Labs around the globe in the first quarter of 2017. The event in Karlsruhe attracted over 6,200 employees, and the attendance and contribution of select customers, partners, start-up companies, SAP Mentors, as well as students on the second day allowed an outside in perspective for SAP employees and insights for SAP's ecosystem. Among the hot topics at this year's event, the Internet of Things (IoT) and Machine Learning gained lots of interest. These areas are also key areas of applying privacy enhancing technologies as they are developed in the publicly funded project PANORAMIX where SAP is a partner in the consortium. SAP's ability and expertise in data security, especially in the field of IoT, and SAP's reputation as a trusted partner to its customers, are of key value for the project. SAP Security Research had its own booth at a highly coveted spot, where the team introduced PANORAMIX to stakeholders within SAP by presenting and demonstrating our research results on anonymization.
Resources spent	0.1 PM
People reached	6200 Industry

Activity	Talk "Talking Behind Your Back - On the Privacy of the Ultrasound Ecosystem"
Location	Mozilla International Privacy Day, London, UK (also streamed)
Date	28 January 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	The talk mainly focused on informing the general public about anonymity networks, and potential threats. The audience was familiar with Tor already, so we used it as an example to inform them about de-anonymization threats, and countermeasures they can employ.
Resources spent	0.05 PM
People reached	100 General Public

Activity	SAP Security Summit
Location	St. Leon-Rot, Germany
Date	14 &15 March 2017
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	We gave a talk on privacy-aware enterprise applications and the use cases enabled by anonymization technologies as pursued in PANORAMIX. Furthermore, we were present at a booth on both days where we presented a demonstration of differential privacy with location data and discussed our research on privacy-preserving methods with visitors and stakeholders.
Resources spent	0.1 PM
People reached	60 Industry

Activity	Meeting with Tor
Location	Amsterdam, The Netherlands
Date	27 & 28 March 2017
Partners involved	GH, UCL, UEDIN, KUL
People involved	Harry Halpin, Claudia Diaz, Tariq Elahi (KUL), Thomas Zacharias (UEDIN)
Relevance to the project	Learning from Tor's experience in practical development of anonymity systems, as well sharing knowledge with various developers interested in mix networking.
Resources spent	0.4 PM
People reached	50 Developers

Activity	Black Hat briefing "OpenCrypto: unchaining the JavaCard ecosystem"
Location	Las Vegas, US (also streamed)
Date	22-27 July 2017
Partners involved	UCL
People involved	Vasilios Mavroudis, George Danezis
Relevance to the project	In this presentation, we present a new cryptographic library for smartcards. Smart cards are already an integral part of many networks (e.g., sim cards in telecommunication networks) but currently developers rely on the limited algorithms that are natively implemented by the card vendors. This severely limits the uses of such cards. Our library is a breakthrough for the smartcard ecosystem, as for the first time it enables developers to implement their own cryptographic algorithms. For instance, with this library smartcards can now be used in mix-nets to guarantee the security of the routing and PKI infrastructure. This work can be combined with our hardware platform to build high-assurance mix-net infrastructure from commercial-off-the-shelf components.
Resources spent	0.1 PM
People reached	800 Industry

Activity	Talk at Def Con 25 "Trojan-tolerant Hardware & Supply Chain Security in Practice"
Location	Las Vegas, US (also streamed)
Date	27-30 July 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	This presentation introduces a novel hardware platform we built with mix-nets use in mind (i.e., it is optimized to perform specific cryptographic operations very fast). More specifically, existing anonymity networks assume that the hardware does not contain intentional or unintentional errors. However, this is not always true. For instance, a broken random number generator may compromise the security of an otherwise reliable system. Our platform, for the first time, enables network administrators to build their infrastructure without placing complete trust on a single chip, but instead allows them to distribute it between many heterogeneous pieces.
Resources spent	0.05 PM
People reached	800 Industry, General Public

Activity	Meeting of European privacy experts
Location	Poland
Date	14 -21 August 2017
Partners involved	CCT
People involved	Moritz Bartl
Relevance to the project	A session on mix-nets and the PANORAMIX mix-net in particular was run. Valuable to the project to get focussed feedback from experts.
Resources spent	0.05 PM
People reached	10 Privacy Experts

2.6 Media Event

Activity	Interview
Media type	Radio - Good Morning Scotland
URL	http://www.bbc.co.uk/programmes/b07xf1b9
Date	11 October 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Engagement with the general public.
Resources spent	0.05 PM
People reached	average audience 500,000 (estimate)

Activity	Media article
Media type	Forbes magazine
URL	https://www.forbes.com/sites/amycastor/2017/08/23/at-crypto-2017-blockchain-presentations-focus-on-proofs-not-concepts/
Date	23 August 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Write up of Aggelos Kiayias presentation at Crypto 2017.
Resources spent	0.05 PM
People reached	6.7M Audience Readership

2.7 Presentations

This section lists dissemination in the form of presentations/talks given by PANORAMIX members at a range of university seminars, national events etc.

Activity	Talk "Science of the Blockchain" at Scottish Enterprise
Location	Edinburgh, UK
Date	28 September 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Dissemination of the ongoing work of the PANORAMIX consortium to an audience of industry representatives in Scotland.
Resources spent	0.05 PM
People reached	75 Industry

Activity:	Joint Latvian-Estonian Theory Days
Location:	Lilaste, Latvia
Type:	Presentation
Date:	13 - 16 October 2016
Involved partners:	UT
People involved:	Helger Lipmaa, Behzad Abdolmaleki, Karim Baghery, Prastudy Fauzi, Janno Siim, Michał Zając
Relevance to the project:	Joint Theory Days gather computer science researchers and PhD students from Estonia and Latvia. The core concept of the event is to disseminate results and share them among scientific community. During the workshop "An Efficient NIZK Shuffle Argument Secure in the Generic Bilinear Group Model" was presented.
Resources spent:	0.3 PM
People reached: about	50 people, computer scientists

Activity	Talk “Secure Decentralized Blockchains without Proofs of Work” at Alan Turing Institute
Location	London, UK
Date	1 November 2016
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Presenting ongoing PANORAMIX research.
Resources spent	0.05 PM
People reached	50 Research and scientific community

Activity	Presentation at KASTEL Seminar at KIT
Location	Karlsruhe Institute of Technology, Germany
Date	10 November 2016
Partners involved	SAP
People involved	Daniel Bernau, Benjamin Weggenmann
Relevance to the project	We gave a presentation for a seminar at KASTEL ("Kompetenzzentrum für angewandte Sicherheitstechnologie") at Karlsruhe University of Technology. The lecture was aimed at graduate students with whom we discussed our current research in PANORAMIX on anonymization and privacy-enhancing technologies as well as our experiences and goals.
Resources spent	0.1 PM
People reached	15 Research and scientific community

Activity	Presentation at Colloquium, University of Trier
Location	University of Trier, Germany
Date	14 December 2016
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	For the colloquium at the Information Security and Cryptography chair at the University of Trier, we gave a presentation of our research in PANORAMIX on data anonymization. The event was aimed at graduate students with whom we discussed the effects and applicability of privacy-preserving technologies.
Resources spent	0.1 PM
People reached	10 Research and scientific community, students

Activity	Talk "On the Privacy and Security of the Ultrasound Ecosystem" at Information Security Seminar, UCL
Location	London, UK
Date	19 January 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	Presented modern threats against anonymity networks. More specifically, we focused on side-channel attacks. The audience was mainly academic with experience in either security or cryptography. In the discussion that followed, we focused on the severity of certain privacy attacks and how they could be combined with other vulnerabilities.
Resources spent	0.05 PM
People reached	30 Research and scientific community

Activity	Talk "On the Privacy and Security of the Ultrasound Ecosystem" at Computer Laboratory Security Seminar
Location	Cambridge, UK
Date	21 February 2017
Partners involved	UCL
People involved	Vasilios Mavroudis
Relevance to the project	We presented modern threats against anonymity networks. More specifically, we focused on side-channel attacks. The audience was purely academic with experience in either security, telecommunications or networks. A discussion followed with very useful insights for our mixnet design.
Resources spent	0.05 PM
People reached	30 Research and scientific community

Activity	Talk at Newcastle University Security Seminar "End-to-end verifiable elections"
Location	Newcastle University, UK
Date	28 February 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Presentation of PANORAMIX related research.
Resources spent	0.05 PM
People reached	25 Research and scientific community

Activity:	Visit to Aarhus University
Location:	Aarhus, Denmark
Type:	Presentation
Date:	21 & 22 February 2017
Involved partners:	UT
People involved:	Prastudy Fauzi (UT)
Relevance to the project:	Presentation of the research ideas on NIZK shuffle arguments that we have constructed in the last 18 months of the project. The audience of the meeting consisted mainly of PhD students and academic researchers. During the presentation we also introduced the project and discussed other possibilities to create secure mix-nets.
Resources spent:	0.05 PM
People reached:	20 Research and scientific community

Activity	Presentation at the CryptoAction Symposium by invitation of EU COST Action Cryptography for Secure Digital Interaction
Location	Amsterdam, the Netherlands
Date	28 March 2017
Partners involved	GH, KUL, UEDIN
People involved	Claudia Diaz (KUL), Harry Halpin (GH), Aggelos Kiayias, Thomas Zacharias (UEDIN)
Relevance to the project	Interaction with the COST Action. PANORAMIX was presented in the talk: "Is Privacy-Enhanced Secure Messaging Possible? The Panoramix Design"
Resources spent	0.2 PM
People reached	25 Research and scientific community

Activity	Ministerial visit to the University of Edinburgh
Location	University of Edinburgh, Informatics Forum
Type	Poster session, oral and video presentation
Date	3 April 2017
Partners involved	UEDIN
People involved	Chris Campbell, Thomas Zacharias
Relevance to the project	Short presentation and discussion of the PANORAMIX workplan and goals with Ben Gummer, Minister for the Cabinet Office, responsible for the Government Digital Service.
Resources spent	0.1 PM
People reached	UK Minister for the Cabinet Office, UK government officials and School of Informatics staff

Activity	Talk: "Blockchain technology: A Secure Solution" at the Edinburgh International Science Festival
Location	Edinburgh, UK
Date	9 April 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	Public engagement, presenting PANORAMIX to the general public.
Resources spent	0.05 PM
People reached	100 General Public

Activity	GI Workshop "Security" and "Legal Framework"
Location	Berlin, Germany
Date	4 May 2017
Partners involved	SAP
People involved	Daniel Bernau, Benjamin Weggenmann
Relevance to the project	We participated in the fourth joint workshop of the working groups "security" and "legal framework" of the "Gesellschaft für Informatik" (GI) with a special focus on anonymization, particularly legal and technical aspects of the new EU data protection regulation (GDPR). We identified and discussed specific issues that arise in the legal context of anonymization technologies. Furthermore, we discussed our research in PANORAMIX on privacy-preserving technologies including mix-nets and differential privacy, which aims towards fulfilling the legal requirements. One result of the discussions was the planning of a joint follow-up event between SAP and legal experts from FZI ("Forschungszentrum Informatik") at Karlsruhe Institute of Technology.
Resources spent	0.1 PM
People reached	30 Research and scientific community, Legal experts, Industry

Activity	The UCL Carnival of Decentralization and Privacy
Location	London, UK
Date	22 May 2017
Partners involved	UCL, KUL, UEDIN
People involved	George Danezis, Claudia Diaz, Aggelos Kiayias
Relevance to the project	1-day meeting hosted by the UCL Information Security group on the theme of anonymous communication, privacy and decentralization to disseminate PANORAMIX and NEXTLEAP findings.
Resources spent	0.15 PM
People reached	75 Research and scientific community

Activity	imec Distributed Trust Workshop on "Data Protection and Privacy"
Location	Leuven, Belgium
Date	20 June 2017
Partners involved	KUL
People involved	Tariq Elahi
Relevance to the project	This talk presented mix networks, the problems they solve, and the still open challenges to wide-scale adoption that the PANORAMIX project aims to meet. The aim of the talk was to promote PANORAMIX to a general lay audience.
Resources spent	0.05 PM
People reached	50 General Public

Activity	Anonymization Workshop with FZI Date: 12.7.2017
Location	Karlsruhe, Germany
Date	12 July 2017
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	As a follow-up event of the GI Workshop "Security" and "Legal Framework", we held a joined workshop with PD Dr. iur. Raabe and legal experts from the "Forschungszentrum Informatik" (FZI) at Karlsruhe Institute of Technology. We discussed the legal interpretation of anonymization in the data privacy law and gave a technical presentation of different privacy definitions, with the goal of finding a common understanding from both legal and technical perspectives. Furthermore, we gave an overview of current anonymization use cases at SAP. Particularly, we presented and discussed our PANORAMIX work package 6 use case and demonstrator.
Resources spent	0.1 PM
People reached	10 Legal experts

2.8 Cross PANORAMIX visits

Activity	Face-to-face meeting of Thomas Zacharias (UEDIN) with the UT team
Location:	Tartu, Estonia
Type:	Presentation and Implementation
Date:	22 - 27 November 2016
Involved partners:	UT, UEDIN
People involved:	Helger Lipmaa (UT), Prastudi Fauzi (UT), Michał Zając (UT), Thomas Zacharias (UEDIN)
Relevance to the project:	Interaction among members from the two partners for the requirements analysis of the PANORAMIX e-voting system and the design of a novel reliable bulletin board
Resources spent:	0.2 PM
People reached	Internal PANORAMIX dissemination

Activity	PANORAMIX Project Steering Committee face to face meeting
Location	BLOOM hotel Brussels
Date	24 January 2017
Partners involved	UEDIN, UCL, UT, UoA, KUL, GH, SAP, GRNET, CCT and External Advisory Board (EAB)
People involved	Aggelos Kiayias, Thomas Zacharias, Mirjam Wester (UEDIN), George Danezis, Ania Piotrowska (UCL), Helger Lipmaa, Michał Zając, Annabell Kuldmaa (UT), Pyrros Chaidos (UoA), Claudia Diaz, Rafael Galvez, Tariq Elahi (KUL), Harry Halpin, Kali Kaneko, Mooness Davarian (GH/LEAP), Benjamin Weggenmann (SAP), Panos Louridas, Dimitris Mitropoulos, Geore Korfiatis, Giorgos Tsoukalas (GRNET), Moritz Bartl (CCT) Bart Preneel, Gus Hosein, Marit Hansen, Omer Tene, Sven Heiberg, Jacques Bus (External Advisory Board)
Relevance to the project	Full day meeting presenting the progress in PANORAMIX to the consortium and EAB. (6 of 8 EAB members were present)
Resources spent	1 PM and €2100 (meeting facilities & catering)
People reached	Internal PANORAMIX dissemination - 27 people

Activity	Implementing Proof of Correct Shuffle in Mix-nets
Location:	Athens, Greece
Type:	Presentation and Implementation
Date:	30 January - 3 February 2017
Involved partners:	UT, UAthens, GRNET
People involved:	Prastudy Fauzi, Janno Siim (UT), Pyrros Chaidos (UoA), Giorgos Korfiatis, Panos Louridas, Dimitris Mitropoulos, Georgios Tsoukalas (GRNET)
Relevance to the project:	Presentation and discussion of the research papers "A Shuffle Argument Secure in the Generic Model" [FLZ16] and "An Efficient Pairing-Based Shuffle Argument" (in submission). Followed by implementation and comparison of the two papers in Python using the bilinear pairing library bplib. The participants consisted of academic researchers and practitioners. The consensus was that the latter paper is the recommended one of the two for creating secure mix-nets.
Resources spent:	0.35 PM
People reached	Internal PANORAMIX dissemination

2.9 Training Courses, Videos and Documentation

Activity	Talk "Cryptography and Voting"
Location	UCL, London, UK
Type	Guest Lecture for "Introduction to Cryptography (COMPGA03)"
Date	12 December 2016
Partners involved	UoA,UCL
People involved	Pyrros Chaidos (UoA)
Relevance to the project	Presented an introduction to cryptographic techniques used to secure internet voting. The presentation discussed the security requirements for holding an election over the internet, and how they differ from other common scenarios. It focused on key cryptographic techniques used to satisfy them. In particular the talk highlighted the use of mixnets to shuffle ballots which is one of the main use cases for PANORAMIX.
Resources spent	0.05 PM
People reached	25 Students

Activity	Video of the core PANORAMIX technology
Type	You tube video: https://www.youtube.com/watch?v=dQtk0NcTseg, also on PANORAMIX website: https://panoramix-project.eu/videos/ and regularly promoted via Twitter.
Date	24 January 2017
Partners involved	Video creation managed by GRNET, with input from all consortium partners.
People involved	Panos Louridas (GRNET)
Relevance to the project	The video is used as a dissemination tool. It describes the core of the PANORAMIX project in animation form and is accessible to a very wide audience.
Resources spent	0.3 PM and €8680
People reached	CPDP 1000, youtube views 500

Activity	BIU Winter School
Location	Bar-Ilan University, Israel
Type	Participation in winter school.
Date	12-16 February 2017
Partners involved	SAP
People involved	Daniel Bernau, Benjamin Weggenmann
Relevance to the project	We attended the 7th BIU Winter School on Cryptography, which focused on the topic of differential privacy. The framework of differential privacy provides a rigorous mathematical treatment of privacy, with concrete provable guarantees that are robust against adversaries with arbitrary computational power and with arbitrary auxiliary knowledge. It is often referred to as "gold standard" in anonymization and its inventors – two of which, namely Kobbi Nissim and Adam Smith, were also giving lectures at the event – have recently been awarded with the Gödel prize. Differential privacy also plays an important part in the PANORAMIX project by supporting and complementing mix-net technology. At this event, we used the possibility to gain better understanding of the differential privacy framework and network with other researchers. Furthermore, we discussed the PANORAMIX goals and vision with other participants to gather feedback on our methodologies
Resources spent	0.2 PM
People reached	20 Research and scientific community.

Activity	Historical Materialism Conference Beirut
Location	Beirut, Lebanon
Type	Presentation
Date	10-12 March 2017
Partners involved	GH
People involved	Harry Halpin
Relevance to the project	Outreach to high-risk activist users
Resources spent	0.25 PM
People reached	30 activists and academics from Middle East, including Turkey, Lebanon, and Iran.

Activity	Guest Lecture at Karlsruhe University of Applied Sciences
Location	Karlsruhe, Germany
Date	20 June2017
Partners involved	SAP
People involved	Benjamin Weggenmann, Daniel Bernau
Relevance to the project	We gave a guest lecture for the Applied Cryptography course at Karlsruhe University of Applied Sciences. The course was aimed at Master's students. We presented different privacy definitions and discussed privacy-enhancing technologies including our research in PANORAMIX.
Resources spent	0.05 PM
People reached	15 Students

Activity	The Summer Research Institute 2017 (SuRI)
Location	Lausanne, Switzerland
Type	Presentation
Date	14-20 June 2017
Partners involved	UCL
People involved	George Danezis
Relevance to the project	SuRI is an annual event that brings together renowned researchers and experts from academia and industry. This year it featured two tracks: 1) Data Science and 2) Security and Privacy. PANORAMIX was represented in the second track with a talk by George Danezis "Foiling on-line surveillance: new developments in anonymous communications and their applications"
Resources spent	0.2 PM
People reached	Scientific community

Activity	The Swiss Blockchain Summer School 2017
Location	Lausanne, Switzerland
Type	Presentation
Date	21-14 June 2017
Partners involved	UEDIN
People involved	Aggelos Kiayias
Relevance to the project	The summer school is an event aimed at bringing together students (Master- and PhD-level), academic researchers, and security experts from industry with an interest in cryptocurrencies and blockchain technology. Kiayias presented "Proving the Security of Blockchain Protocols: From Proof of Work to Proof of Stake"
Resources spent	0.2 PM
People reached	Scientific community

Activity	2nd Hebrew University Networking Summer
Location	Jerusalem, Israel
Type	Presentation
Date	18, 20-22 June 2017
Partners involved	UCL
People involved	George Danezis
Relevance to the project	PANORAMIX research was included in George's tutorial "Foiling on-line surveillance: new developments in anonymous communications and their applications". The event was attended by networking researchers from the United States, Europe and Israel.
Resources spent	0.1 PM
People reached	Scientific community

3. Progress monitoring

The key performance indicators (KPI), with yearly targets, and the total actual activity for all partners are found in Table 3.1. Overall targets have been met with some even substantially surpassed. Especially the large number of publications at research conferences and in research journals are a testament to the outstanding research that is being carried out in PANORAMIX as all these are peer-reviewed publications.

Two new categories have been added –in this report– to our list of dissemination activities since the previous Dissemination Report, namely "Presentations" (16) and "Cross PANORAMIX visits" (3). These two have not been added to the list of KPIs as no targets have been previously set, however, they have turned out to be an important and valuable form of dissemination within the project.

Dissemination Type	Actual	Target (per year)
User-facing website articles and blog posts	16	12
Industry Event	10	6
Policy Conference	2	3
Media Event	2	2
Research Conference Publications	15	6
Research Journal Publications	4	3
Training Courses, Videos & Documentation	8	3

Table 3.1: Dissemination Key Performance Indicators

Bibliography

[AIKM16] Ioannis G. Askoxylakis, Sotiris Ioannidis, Sokratis K. Katsikas, and Catherine A. Meadows, editors. *Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part I*, volume 9878 of *Lecture Notes in Computer Science*. Springer, 2016.

[AKTZ17] Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, and Thomas Zacharias. MCMix: Anonymous messaging via secure multiparty computation. In *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC, 2017.

[ASJ+16] George Argyros, Ioannis Stais, Suman Jana, Angelos D. Keromytis, and Aggelos Kiayias. SFADiff: Automated evasion attacks and fingerprinting using black-box differential automata learning. In Weippl et al. [WKK+16], pages 1690–1701.

[BBK17] Jonas Böhler, Daniel Bernau, and Florian Kerschbaum. Privacy-preserving outlier detection for data streams. In Giovanni Livraga and Sencun Zhu, editors, *Data and Applications Security and Privacy XXXI: 31st Annual IFIP WG 11.3 Conference, DBSec 2017, Philadelphia, PA, USA, July 19-21, 2017, Proceedings*, pages 225–238, Cham, 2017. Springer International Publishing.

[BBL17] Fabrice Benhamouda, Florian Bourse, and Helger Lipmaa. CCA-Secure inner-product functional encryption from projective hash functions. In Fehr [Feh17], pages 36–66.

[BKZZ16] Foteini Baldimtsi, Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. Indistinguishable proofs of work or knowledge. In Cheon and Takagi [CT16], pages 902–933.

[CHJ17] Giovanni Cherubin, Jamie Hayes, and Marc Juárez. Website fingerprinting defenses at the application layer. *PoPETs*, 2017(2):186–203, 2017.

[CT16] Jung Hee Cheon and Tsuyoshi Takagi, editors. *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, 2016.

[Feh17] Serge Fehr, editor. *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II*, volume 10175 of *Lecture Notes in Computer Science*. Springer, 2017.

[FLZ16] Prastudy Fauzi, Helger Lipmaa, and Michał Zając. A shuffle argument secure in the generic model. In Cheon and Takagi [CT16], pages 841–872.

[GKL17] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol with chains of variable difficulty. In Katz and Shacham [KS17], pages 291–323.

[JIP+16] Marc Juárez, Mohsen Imani, Mike Perry, Claudia Díaz, and Matthew Wright. Toward an efficient website fingerprinting defense. In Askoxylakis et al. [AIKM16], pages 27–46.

[KLT16] Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis. Practical non-malleable codes from l-more extractable hash functions. In Weippl et al. [WKK+16], pages 1317–1328.

[KOR+16] Aggelos Kiayias, Ozgur Oksuz, Alexander Russell, Qiang Tang, and Bing Wang. Efficient encrypted keyword search for multi-user data sharing. In Askoxylakis et al. [AIKM16], pages 173–195.

[KRDO17] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Katz and Shacham [KS17], pages 357–388.

[KS17] Jonathan Katz and Hovav Shacham, editors. *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*. Springer, 2017.

[KZZ17a] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. Auditing for privacy in threshold PKE e-voting. *Inf. & Comput. Security*, 25(1):100–116, 2017.

[KZZ17b] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. Ceremonies for end-to-end verifiable elections. In Fehr [Feh17], pages 305–334.

[KZZ17c] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. An efficient E2E verifiable e-voting system without setup assumptions. *IEEE Security & Privacy*, 15(3):14–23, 2017.

[Lip17] Helger Lipmaa. Optimally sound sigma protocols under DCRA. In *21st International Conference on Financial Cryptography and Data Security 2017*, Malta, 2017.

[LP17] Helger Lipmaa and Kateryna Pavly. A simpler rate-optimal CPIR protocol. In *21st International Conference on Financial Cryptography and Data Security 2017*, Malta, 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. *PoPETs*, 2017(2):95–112, 2017.

[PHE+17] Ania Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The Loopix anonymity system. In *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC, 2017. USENIX Association.

[WKK+16] Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. ACM, 2016.