Tariq Elahi & Rafael Galvez—Eds. (KUL)
George Danezis (UCL)
Claudia Diaz (KUL)
Harry Halpin (GH)
Florian Kerschbaum (SAP)
Aggelos Kiayias (UEDIN)
Helger Lipmaa (UT)
Panos Louridas (GRNET)
Anna Piotrowska (UCL)
Benjamin Weggenmann (SAP)
Michal Zajac (UT)

Dissemination Report I

Deliverable D2.3

31st October 2016
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2016-07-25	TE (KUL)	Initial draft
0.1	2016-08-26	TE (KUL)	Incorporated partners' dissemination activities
1.0	2016-08-29	TE,RG (KUL)	Final editing and review
1.0	2016-08-31	AK (UEDIN)	Final version and submission to the EC
1.1	2016-10-16	TE, RG (KUL)	Revision after 1st periodic review
1.2	2016-10-19	RG (KUL)	Add people involved, relevance to the project and resources spent
1.2	2016-10-24	MW (UEDIN)	Reviewed and provided feedback
1.2	2016-10-26	RG (KUL)	Revision after review
1.3	2016-10-28	RG (KUL)	Revision after second review
2.0	2016-10-31	AK (UEDIN)	Revised final version and submission to the EC

Executive Summary

This dissemination report, the first of three, encompasses the dissemination activities of the project partners for the time period from September 2015 through to August 2016. 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 the targeted number of outputs.

Contents

1. Introduction

This chapter states the purpose of the Dissemination Report of the first 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 2015 through to August 2016. 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 (D2.3) 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, D2.3 is closely related to the following WP2 deliverables:

- Deliverable #20: D2.1-Public Web Page and Blog [UEDIN]
- Deliverable #21: D2.2-Dissemination plan [KUL]
- Deliverable #23: D2.4-Standardization Report [GH]
- Deliverable #24: D2.5-Preliminary Exploitation Plan [SAP]
- Deliverable #25: D2.6-Complete Exploitation Plan [GRNET]
- Deliverable #26: D2.7-Report on Exploitation Activities and Updated Plan for Further Exploitation [GH, MV]
- Deliverable #27: D2.8-Scientific Advisory Board Reports [UT]
- Deliverable #28: D2.9-Dissemination Report II [KUL]
- Deliverable #29: D2.10-Dissemination Report III [KUL]

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 and blog posts

Activity	A technical reading of the "HIMR Data Mining Research Problem Book"
Location	https://conspicuouschatter.wordpress.com/2016/02/03/a-technical-reading-of-the-himr-data-mining-research-problem-book/
Date	February 3rd, 2016
Type	Blog post
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	This post summarises the technical content of the leaked report from GCHQ relating to open problems and infrastructures involved in its surveillance operations. Such technical details provide PANORAMIX and its partners a better understanding of the threat models which strong privacy technologies may have to withstand; standard interception equipment capabilities and procedures surrounding them; and the economics of scalling network surveillance up. As such it provides the scientific community, and the wider public, a better understanding of the extend and cost at which network adversaries (GCHQ but also others technologically advanced states) can perform pervasive surveillance. The post has been visited over 3000 times. Target groups: Research and scientific community, and Wider public.
Resources spent	0.5 PM for the background reading on mass surveillance infrastructures. 0.1 PM for the post itself.

Activity	Zero-knowledge proofs library in petlib
Location	https://conspicuouschatter.wordpress.com/2016/01/23/zero-knowledge-proofs-library-in-petlib/
Type	Blog post
Date	January 23rd, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	The blog post introduces petlib - a python cryptographic library that implements a number of Privacy Enhancing Technologies. This post introduces the facilities petlib provides to build zero-knowledge proofs, a key PANORAMIX building blog. The post was written as part of sharing this information, and the technical knowhow of using these technologies, within the UCL group, and has been shared with the wider scientific and engieering community. Target groups: Research and scientific community, and Wider public.
Resources spent	0.1 PM were spent by Danezis (UCL) to write the post

Activity	Notes on Scrambling for Safety 2016 Session 1
Location	https://conspicuouschatter.wordpress.com/2016/01/07/notes-on-scrambling-for-safety-2016-session-1/
Type	Blog post
Date	January 7th, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	The blog post summarizes for wide public the first session of "Scrambling for Safety 2016" meeting, an event organized to discuss the most current issues in UK information policy, related this time to the draft of the Investigatory Powers Bill. The event described legislative changes in the UK, that allow for mass foreign meta-data collection, and equipment interference – both of which contribute ot our understanding of the threat model privacy enhancing technologies may have to operate in and withstand. The reports are notes from the meetings, that are made avvailable to the wider community and those that were not present. Target groups: Research and scientific community, and Wider public.
Resources spent	0.1 PM attending the event (Danezis) and 0.5 PM to gain the understanding of the context of the legislation.

Activity	Notes on Scrambling for Safety 2016 Equipment Interference Session
Location	https://conspicuouschatter.wordpress.com/2016/01/07/notes-on-scrambling-for-safety-2016-equipment-interference-session/
Type	Blog post
Date	January 7th, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	The blog post summarizes for wide public the first session of "Scrambling for Safety 2016" meeting, an event organized to discuss the most current issues in UK information policy, related this time to the draft of the Investigatory Powers Bill. The event described legislative changes in the UK, that allow for mass foreign meta-data collection, and equipment interference – both of which contribute ot our understanding of the threat model privacy enhancing technologies may have to operate in and withstand. The reports are notes from the meetings, that are made avvailable to the wider community and those that were not present. Target groups: Research and scientific community, and Wider public.
Resources spent	0.1 PM to attend event (Danezis) and 0.5 PM to understand the context of the legislation.

Activity	The Social Construction of Trust in Cryptographic Systems
Location	https://conspicuouschatter.wordpress.com/2016/02/03/the-social-construction-of-trust-in-cryptographic-systems/
Type	Blog post
Date	February 3rd, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	This blog post summarises the trust related assumption, and resoning, related to building high assurance systems such as PANORAMIX to a lay audiance. Target groups: Wider public.
Resources spent	0.25 PM (Danezis) to write this section of the chapter. 0.1 PM to convert it into a post (Danezis).

Activity	Public policy debates around cyber-investigations laws in the UK
Location	https://panoramix-project.eu/public-policy-debates-around-cyber-investigations-laws-in-the-uk/
Type	Blog post
Date	January 11st, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	This blog post summarises, on the PANORAMIX website, all the UCL research group, posts and articles relating to surveillance policy in the UK. Those debates have a material impact on technologies such as PANORAMIX that try to defeat technical interception caapbilities, and hide meta-data despite them – particularly if they are performed by a non-authorised third party or country.
Resources spent	0.1 PM to write the post (Danezis)

Activity	Privacy-preserving Empirical Data Collection For Anonymous Communication Systems
Location	https://securewww.esat.kuleuven.be/cosic/?p=4690
Type	Blog post
Date	April 21st, 2016
Involved partners	KU Leuven
People involved	Tariq Elahi (KUL)
Relevance to the project	This blog post provides guidance to collect data to conduct experiments on PANORAMIX and other related anonymous communications systems, without compromising the safety of their users.
Resources spent	0.1 PM to write the post (Elahi)

Activity	PANORAMIX: Our Goals
Location	https://panoramix-project.eu/panoramix-overview/our_goals/
Type	Website article
Date	December 1st, 2015
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	It recaps the project's objectives in order to make them available to a wide audience via our web-site.
Resources spent	approx. 0 PM to write the blog post.

Activity	Blockchain technologies summer school
Location	https&//panoramix-project.eu/blockchain-technologies-summer-school/
Date	May 30th, 2016
Involved partners	UEDIN, UCL, GH
People involved	Aggelos Kiayias (UEDIN), George Danezis (UCL), Harry Halpin (GH)
Relevance to the project	The blockchain summer school was a very successful event with more than 150 participants that received training in blockchain technologies and it was important to communicate the participation of three of the project consortium members (with two of them, Aggelos, George giving invited talks).
Resources spent	approx. 0 PM to write the blog post.

Activity	PANORAMIX Project Steering Committee - 2nd face to face meeting
Location	https&//panoramix-project.eu/panoramix-project-steering-committee-march-21st-2016/
Date	March 21st, 2016
Involved partners	UEDIN,UCL,UT,UoA,KUL,GH,Mobile Vikings,SAP, GRNET
People involved	Aggelos Kiayias (UEDIN); Anna Piotrowska (UCL); Athanasios Angelakis (UoA); Benjamin Weggenman (SAP); Florian Kerschbaum (SAP); Giorgos Tsoukalas (GRNET); Harry Halpin (GH); Helger Lipmaa (UT); Jacques Bus (External Advisory Board); Joss Wright (Ethics Advisor); Michal Zajac ; Panos Louridas (GRNET); Rafael Galvez (KUL); Sacha van Geffen (GH); Sven Heiberg (External Advisory Board); Tariq Elahi (KUL).
Relevance to the project	The project steering committee is arranged quarterly and is face to face every six months. The blog posts details the meeting proceedings.
Resources spent	approx. 0 PM to write the blog post.

Activity	PANORAMIX members participate in high level privacy conference, “ Protecting online privacy by enhancing IT security and strengthening EU IT capabilities’
Location	https://panoramix-project.eu/panoramix-members-participate-in-high-level-privacy-conference/
Type	Blog post
Date	December 18th, 2015
Involved partners	UEDIN, UCL.
People involved	Aggelos Kiayias (UEDIN), George Danezis (UCL).
Relevance to the project	Relevant to communicate to a wide audience the involvement of two consortium members to this influential meeting. Both Aggelos and George provided white papers on privacy that were posted on the conference’s web-site.
Resources spent	approx. 0 PM to write the blog post.

Activity	PANORAMIX comments on David Chaums new mix-net system
Location	https://panoramix-project.eu/panoramix-comments-about-david-chaums-new-cmix-system/
Type	Blog post
Date	January 22nd, 2016
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	Important to publicise that after a hiatus of many years in mix-net research, their inventor comes back with a novel proposal, and the consortium coordinator is interviewed to provide comments on this design.
Resources spent	approx. 0 PM to write the blog post. 0.25PM to thoroughly review cMIX.

2.2 Research Conference

Activity	20th European Symposium on Research in Computer Security (ESORICS 2015)
Type	Conference presentation and publication
Location	Vienna, Austria
Date	September 21-25, 2015
Involved partners	SAP
People involved	Florian Kerschbaum (SAP)
Relevance to the project	Florian Kerschbaum gave a presentation on "Privacy-Preserving Observation in Public Spaces" [GRZ+15]. Target group: Research and scientific community.
Resources spent	0.28 PM

Activity	RSA Conference Cryptographers' Track, 2016.
Type	Conference presentation and publication
Location	San Francisco, CA, USA
Date	February 29-March 4, 2016
Involved partners	UT
People involved	Helger Lipmaa (UT)
Relevance to the project	The presentation of "Efficient Culpably Sound NIZK Shuffle Argument without Random Oracles" [FL16] has taken place during annual RSA Conference Cryptographers' Track (CT-RSA) that gathers both industry and academic community focused on cryptography and security. The meeting was used to promote PANORAMIX project idea and to present to the audience recent research problems along with propositions of solutions. Conference was also used to transfer PANORAMIX know-how to the audience.
Resources spent	0.4 PM

Activity	8th International Conference on Cryptology in Africa — AFRICACRYPT
Type	Conference presentation and publication
Location	Fes, Morocco
Date	April 13-15, 2016
Involved partners	UT
People involved	Helger Lipmaa (UT)
Relevance to the project	The presentation of "Prover-Efficient Commit-And-Prove Zero-Knowledge SNARKs" [Lip16] has taken place during annual Africacrypt conference. The event gathers both industry and academic community focused on cryptography and security. During the meeting, PANORAMIX project idea has been promoted and mix-net know-how disseminated.
Resources spent	0.25 PM

Activity	ACM Conference on Computer and Communications Security — CCS 2015
Type	Conference presentation and publication
Location	Denver, CO, USA
Date	October 12-16, 2015
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	HORNET [CAB+15] introduces a novel high-speed anonymous system based on onion routing, which can be used as design option for PANORAMIX low-latency anonimization. The design was presented during ACM CCS 2015, which allowed to discuss with the research community the main project objectives (particularly Objective 1) and the ideas and following benefits for anonymous communication resulting from the PANORAMIX project. Target group: Research and scientific community.
Resources spent	0.5 PM (Danezis) writing and copy editing the final paper for submission.

Activity	USENIX Security 2016
Type	Conference presentation and publication
Location	Austin, TX, USA
Date	August 10-12, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	The paper " k-fingerprinting: a Robust Scalable Website Fingerprinting Technique" [HD16] presented during USENIX 2016 discusses a new technique of conducting the fingerprinting attacks with a better performance than the existing state of the art attacks. The contribution of this paper discussed with the research community allows to spread the awareness about potential risks for the anonymity systems and discuss the possible designs of defenses in PANORAMIX project, which are not developed in current existing systems. Target group: Research and scientific community.
Resources spent	0.25 (Danezis) writing the paper, and preparing presentation material.

Activity	Network and Distributed System Security Symposium 2016
Type	Conference presentation and publication
Location	San Diego, CA, USA
Date	February 21-24, 2016
Involved partners	UCL
People involved	George Danezis (UCL)
Relevance to the project	The design of the new techniques used for privacy preserving gathering of large scale statistics, presented during NDSS 2016 under the title " Efficient Private Statistics with Succinct Sketches" [MDC16], allowed to discuss the large need of the development of the differential privacy mechanisms for mix-network based applications, which is one of the PANORAMIX project objectives, and present the possible solution developed by the PANORAMIX project. Target group: Research and scientific community.
Resources spent	0.25 PM (Danezis) writing the paper, and preparing presentation material.

Activity	When owl:sameAs isn't the Same Redux: Towards a Theory of Identity, Context, and Inference on the Semantic Web [HHT15]
Type	Conference presentation and publication
Location	Larnaca, Cyprus
Date	November 2-6, 2015
Involved partners	GH
People involved	Harry Halpin (GH)
Relevance to the project	The talk addresses the topic of inference in context, i.e. how new contexts can enable new kinds of inference that may reveal crucial identiying information. This has long been a problem for contextual integrity theories in privacy, as put forward by Nissenbaum. Target group: Research and scientific community.
Resources spent	1 PM writing the paper, and preparing presentation material.

Activity	ACM Conference on Electronic Commerce — EC 2016
Type	Conference presentation and publication
Location	Maastricht, The Netherlands
Date	July 24-28, 2016
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	Since 1999 the ACM Special Interest Group on Electronic Commerce (SIGecom) has sponsored the leading scientific conference on advances in theory, systems, and applications at the interface of economics and computation, including applications to electronic commerce. The ACM EC conference is an important dissemination venue aligned with the project objectives. We presented results, "Blockchain Mining Games" [KKKT16] that were developed in the first year WP3 effort.
Resources spent	Conference participation and publication costs.

Activity	IEEE European Security & Privacy Conference 2016.
Type	Conference presentation and publication
Location	Maastricht, The Netherlands
Date	March 21-24, 2016
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	The IEEE EURO S&P is a new venue that is related (and meant to be a European counterpart) to the IEEE Security & Privacy conference that takes place in Oakland, CA, USA each year in May. The first edition was very successful in terms of participation and the involvement of consortium members in the programme of the conference was a great dissemination opportunity for the project and we presented our work "Highly-Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet" Online) [JKKX16] .
Resources spent	Conference participation and publication costs.

2.3 Research Journal

Activity	SoK: Making Sense of Censorship Resistance Systems [KES+16]
Type	Journal
Date	July 14th, 2016
Involved partners	KUL
People involved	Tariq Elahi (KUL)
Relevance to the project	the paper conducted a comprehensive survey of deployed Censorship Resistance Systems as well as those discussed in academic literature- to systematize censorship resistance systems by their threat model and corresponding defenses. It provides PANORAMIX with guidelines to defense different types of censor adversaries. Target group: Research and scientific community.
Resources spent	0.5 PM writing the paper, and preparing presentation material.

Activity	A Framework for the Game-theoretic Analysis of Censorship Resistance [EDH+16]
Type	Journal
Date	July 14th, 2016
Involved partners	KUL
People involved	Tariq Elahi (KUL)
Relevance to the project	the paper describes a general framework for exploring and identifying optimal strategies for the censorship circumventor, in order to maximize the amount of CRS traffic not blocked by the censor. PANORAMIX can exploit this framework to tailor its defenses against existing censors. Target group: Research and scientific community.
Resources spent	0.5 PM writing the paper, and preparing presentation material.

2.4 Policy Conference

Activity	European Parliament meeting
Location	Brussels, Belgium
Date	February 20th, 2016
Involved partners	GH
People involved	Sacha Van Geffen (GH), Deborah Meibergen (GH), and Harry Halpin (GH)
Relevance to the project	Visited the European Parliament (Brussels) to discuss upcoming cybersecurity directives and its relationship to PANORAMIX, as well as possible future events at the European Parliament. Target group: Governmental Bodies.
Resources spent	0.1 PM

Activity	Workshop PL3 - From cybersecurity to terrorism - are we all under surveillance?
Location	Brussels, Belgium
Date	June 8-10, 2016
Involved partners	GH
People involved	Sacha Van Geffen (GH)
Relevance to the project	Attended the EuroDIG "Workshop PL3 - From cybersecurity to terrorism - are we all under surveillance?" and discussed the policies around the importance of open-source and securing end-users, not just organizations, in terms of cybersecurity and spread awareness of the goals of PANORAMIX. Target groups: Governmental Bodies and Wider Public.
Resources spent	0.1 PM

Activity	United Nations Internet Governance Forum 2015
Location	Joo Pessoa, Brazil
Date	November 10-13, 2015
Involved partners	GH
People involved	Harry Halpin (GH)
Relevance to the project	Presentation on "The Right to Protest Online" Other participants on the panel were Gabrielle Guillemin from Article 19, Eleonora Rabinovich from Google, Elvana Thaci from the Council of Europe. The presentation discussed how Article 11 of the European Convention on Human Rights applies to the internet, and the role of new technologies such as mix networking in PANORAMIX ran by SMEs like Greenhost to enable human rights in repressive environments. Target groups: Governmental Bodies, Wider Public, and Industry.
Resources spent	0.2 PM

2.5 Industry Event

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

Activity	International Workshop on Inference and Privacy in a Hyperconnected World 2016
Location	Darmstadt, Germany.
Type	Presentation "Deanonymizing Social Networks using Machine Learning"
Date	July 18, 2016
Involved partners	(UCL)
People involved	George Danezis (UCL)
Relevance to the project	This talk presented challenges relating to de-anonymizing users of anonymized datasets using machine learning attacks. The objective of PANORAMIX is to provide a higher level of protection, and defeat such attacks, thus protecting privacy in a stronger sense. The talk was the keynote speech in the 'Inference and Privacy' workshop associated with the Privacy Enhancing Symposium in 2016, and was attended by over 50 key researchers and industry in the field of perivacy technologies and machine learning / inference. Target group: Research and scientific community.
Resources spent	0.1 PM

Activity	3rd OpenPGP email summit
Location	Dreieich, Germany
Date	July 9-10, 2016
Involved partners	GH
People involved	Ruben Pollan (Grenhost)
Relevance to the project	In this meeting, the work of PANORAMIX on the LEAP platform was presented to an audience of developers as well as German secure services providers who may want to deploy PANORAMIX. There was discussions of future standardization with IETF OpenPGP co-chair Daniel Kahn Gilmour. Target groups: Security and privacy providers, and Industry.
Resources spent	0.2 PM

Activity	Europython 2016
Location	Bilbao, Spain
Date	July 17-24, 2016
Involved partners	GH
People involved	Kali Kalineko (GH)
Relevance to the project	PANORAMIX's work on the LEAP code was presented to the larger European Python developer community. This solicited more open source involvement in PANORAMIX from outside the project partners. Target groups: Security and privacy providers, and Industry.
Resources spent	0.2 PM

Activity	Les Entretiens du nouveau monde industriel (ENMI) 2015.
Location	Paris, France
Date	November 10-13, 2015
Involved partners	GH
People involved	Harry Halpin (GH)
Relevance to the project	Harry Halpin gave a presentation on "Architecture, traces et modles de valeur" on the role of privacy in next-generation Internet technologies, as exemplified by the work of PANORAMIX on the LEAP codebase. Other participants included Christian Faur (Octo technologies) and Pierre Guehenneux (Vinci construction). Target groups: Industry and Wider public.
Resources spent	0.5 PM

Activity	LEAP gathering
Location	Sao Paulo, Brazil
Type	Hackathon
Date	April 20-28, 2016
Involved partners	GH
People involved	Ruben Pollan (GH), Kali Kalineko (GH)
Relevance to the project	In this meeting, Greenhost got to meet other developers from external collaborators and possible future customers like Thoughtworks. Greenhost developers worked very intensely for a week with Thoughtworks at their Brazilian office and a unified vision of what kinds of services Thoughtworks would be interested in purchasing that could be developed by PANORAMIX was achieved, as well as many practical changes to the codebase. Target groups: Security and privacy providers, and Industry.
Resources spent	1.0 PM

Activity	Hackathon KoWa
Location	Freiburg, Germany and Waltershausen, Germany
Type	Hackathon
Date	July 5-16, 2016
Involved partners	GH
People involved	Ruben Pollan (GH), Kali Kaneko (GH)
Relevance to the project	In this meeting, the programmers working on LEAP software for Greenhost worked intensively for a week, jointly with other programmers (Holger Krekel and Max Wiehle) working on encrypted email from the NEXTLEAP EC project. This meeting led the groundwork for future co-operation between the two projects. Target groups: Research and scientific community and Industry.
Resources spent	0.5 PM

Activity	E-enabled elections in Estonia: Forum on research and development in 2015, https://cyber.ee/en/news/e-enabled-elections-in-estonia-forum-on-research-and-development-in-2015/
Location	Tartu, Estonia
Type	Presentation “Privacy and Accountability in Networks via Optimized Randomized Mixnets”
Date	November 5-6, 2015
Involved partners	UT
People involved	Helger Lipmaa (UT)
Relevance to the project	The meeting was focused on presenting results of research on Estonian verifiable internet voting both from the technical and sociological side. We introduced the concept of mixnet and the PANORAMIX project in general to the audience of the meeting consisting of security experts from both industry (external to the consortium) and academic community and government representatives responsible for the Estonian e-voting system. Target group: Research and scientific community and Industry.
Resources spent	0.06 PM

2.6 Media event

Activity	The Father of Online Anonymity Has a Plan to End the Crypto War
Location	Wired magazine: https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/
Date	January 6th, 2016
Type	Media article
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	We provided commentary and answered questions regarding privacy preserving systems to the Wired journalist writing an article about cMIX. cMIX is a relevant new mix-net system devised by David Chaum, the inventor of mix-nets and member of our external advisory board.
Resources spent	0.1 PM

Activity	David Chaum's cMix: New tool for anonymity on the Internet
Location	TechTarget magazine http://searchsecurity.techtarget.com/news/4500271269/David-Chaums-cMix-New-tool-for-anonymity-on-the-Internet
Date	January 19th, 2016
Type	Media article
Involved partners	UEDIN
People involved	Aggelos Kiayias (UEDIN)
Relevance to the project	We provided commentary and answered questions regarding privacy preserving systems to the Techtarget journalist writing an article about cMIX. cMIX is a relevant new mix-net system devised by David Chaum, the inventor of mix-nets and member of our external advisory board.
Resources spent	0.1 PM

2.7 Training Courses, Videos and Documentation

Activity	A Survey on Routing in Anonymous Communication Protocols [SSA+16]
Type	Technical Report
Date	August 19th, 2016
Involved partners	KUL
People involved	Claudia Diaz (KUL)
Relevance to the project	the report surveys previous research on designing, developing, and deploying systems for anonymous communication. This understanding allows PANORAMIX to explore the consequences of different design options the project needs to make. Target group: Research and community.
Resources spent	0.1 PM

Activity	AWARE: Anonymization With guARanteEd privacy
Type	Technical Report
Date	2016
Involved partners	SAP
People involved	Florian Kerschbaum (SAP)
Relevance to the project	We analyzed the specific technical challenges in anonymization and evaluated a set of differentially private mechanisms for different use cases. The results were and still are used to raise awareness for differential privacy within SAP and to promote its benefits and indicate possible areas of application to potential stakeholders. Furthermore, we identified areas of interest for further research. Target group: Industry.
Resources spent	1 PM

Activity	Summer school on Secure and Trustworthy Computing
Location	Bucharest, Romania
Type	Summer school
Date	September 23-27, 2015
Involved partners	SAP
People involved	Daniel Bernau (SAP)
Relevance to the project	At this event we used the possibility to network with other privacy related EU Projects and exchange on methodologies. Furthermore, we discussed the PANORAMIX goals and vision with other participants to gather feedback. Target group: Research and scientific community.
Resources spent	0.28 PM

Activity	Bar-Ilan University Computer Science Colloquium
Location	Bar-Ilan University, Tel-Aviv Israel
Type	Presentation
Date	December 10th, 2015
Involved partners	GH
People involved	Harry Halpin (GH)
Relevance to the project	Presentation on "Emerging Standards for Cryptography", including demonstrating the LEAP codebase and describing the cost/benefits of mix-networking solutions like PANORAMIX with Amir Herzberg's research on AnonBox that also applies mix-networking to messaging. Target group: Research and scientific community.
Resources spent	0.2 PM

Activity	Beirut Institute for Critical Analysis and Research
Location	Beirut, Lebanon
Type	Presentation
Date	August 25, 2016
Involved partners	GH
People involved	Harry Halpin (GH)
Relevance to the project	Presentation on "The Origins and Future of Surveillance" where he discussed privacy-enhancing technologies with human rights defenders from groups such as Gulf Humans Rights Watch. The talk included both a broad historical overview and basics such as threat models, and compared mix-networking solutions to better known onion-routing solutions like Tor. Target group: Wider public.
Resources spent	0.2 PM

Activity	The Summer Research Institute 2016 Security/Privacy Edition
Location	Lausanne, Switzerland
Type	Presentation
Date	June 20-24 2016
Involved partners	UT, UEDIN
People involved	Helger Lipmaa (UT), Aggelos Kiayias (UEDIN)
Relevance to the project	Presentation "Efficient Culpably Sound NIZK Shuffle Argument Without Random Oracles". The audience of the meeting consisted mainly of PhD students and academic researchers. During the presentation we introduced project's idea and outcomes to the audience and promoted research solutions that meet open questions considering secure mix-nets. Target group: Research and scientific community.
Resources spent	0.3 PM. Travel costs covered by SuRI.

Activity	6th Crypto.Sec Day
Location	Athens, Greece
Type	Presentation
Date	July 18th, 2016
Involved partners	UT, UEDIN, GRNET
People involved	Helger Lipmaa (UT), Aggelos Kiayias (UEDIN), Thomas Zacharias (UEDIN), Panos Louridas (GRNET), Giorgos Tsoukalas (GRNET)
Relevance to the project	Presentation "Efficient Culpably Sound NIZK Shuffle Argument Without Random Oracles". The audience of the meeting consisted of students (undergraduates, graduates and PhD) and academic researchers. During the presentation we introduced project's idea and outcomes to the audience and promoted research solutions that meet open questions considering secure mix-nets. Target group: Research and scientific community.
Resources spent	0.15 PM. Travel costs covered by COST IC306 action Cryptography.

Activity	Blockchain technologies summer school
Location	Athens, Greece
Type	Training course
Date	May 29 - June 3, 2016
Involved partners	UEDIN, UCL, GH
People involved	Aggelos Kiayias (UEDIN), George Danezis (UCL), Harry Halpin (GH).
Relevance to the project	We co-organised and participated in the IACR summer school on blockchain technologies. The school was a major event in the area of blockchain systems that has high relevance to privacy and the goals of the PANORAMIX consortium. The event was one of the most successful IACR summer schools that numbered more than 150 participants.
Resources spent	0.75 PM. Travel costs covered by school organisation.

3. Progress monitoring

The key performance indicators, with yearly targets, and the total actual activity for all partners are found in Table 3.1. The dissemination activities exceeded the targets in all channels except the "Research Journal" channel, where two articles were accepted in the reporting period while the hope was for three.

Dissemination Type	Actual	Target (per year)
User-facing website articles and blog posts	13	12
Industry Event	7	6
Policy Conference	3	3
Media Event	2	2
Research Conference	9	6
Research Journal	2	3
Training Courses, Videos, and Documentation	7	3

Table 3.1: Dissemination Key Performance Indicators

Bibliography

[CAB+15] Chen Chen, Daniele Enrico Asoni, David Barrera, George Danezis, and Adrian Perrig. HORNET: high-speed onion routing at the network layer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, pages 1441–1454, 2015.

[EDH+16] Tariq Elahi, J Doucette, Hadi Hosseini, S Murdoch, and Ian Goldberg. A framework for the game-theoretic analysis of censorship resistance. volume 4, pages 83–101. 2016.

[FL16] Prastudy Fauzi and Helger Lipmaa. Efficient culpably sound nizk shuffle argument without random oracles. In Kazue Sako, editor, *Topics in Cryptology - CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, pages 200–216. Springer International Publishing, Cham, 2016.

[GRZ+15] Chaowen Guan, Kui Ren, Fangguo Zhang, Florian Kerschbaum, and Jia Yu. Symmetric-key based proofs of retrievability supporting public verification. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 203–223. Springer, 2015.

[HD16] Jamie Hayes and George Danezis. k-fingerprinting: a robust scalable website fingerprinting technique. *USENIX Security Symposium 2016*, August 2016.

[HHT15] Harry Halpin, Patrick J. Hayes, and Henry S. Thompson. When owl:sameas isn't the same redux: Towards a theory of identity, context, and inference on the semantic web. In Henning Christiansen, Isidora Stojanovic, and A. George Papadopoulos, editors, *Modeling and Using Context: 9th International and Interdisciplinary Conference, CONTEXT 2015, Larnaca, Cyprus, November 2-6,2015. Proceedings*, pages 47–60. Springer International Publishing, Cham, 2015.

[JKKX16] Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In *IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrücken, Germany, March 21-24, 2016*, pages 276–291, 2016.

[KES+16] Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M Swanson, Steven J Murdoch, and Ian Goldberg. Sok: Making sense of censorship resistance systems. In *Proceedings on Privacy Enhancing Technologies*, volume 4, pages 37–61. De Gruyter, 2016.

[KKKT16] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, pages 365–382, New York, NY, USA, 2016. ACM.

[Lip16] Helger Lipmaa. Prover-efficient commit-and-prove zero-knowledge snarks. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2016: 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, pages 185–206. Springer International Publishing, Cham, 2016.

[MDC16] Luca Melis, George Danezis, and Emiliano De Cristofaro. Efficient private statistics with succinct sketches. In *23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016.

[SSA+16] Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Diaz. A survey on routing in anonymous communication protocols. Technical report, KU Leuven Technical Report, 2016.