Harry Halpin–Ed. (GH)

Standardisation Report

Deliverable D2.4

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

Dissemination Level: Public

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2018-12-05	HH (GH)	Initial draft
0.2	2018-12-12	RG (KUL)	Review and proofreading
0.3	2019-01-07	HH (GH)	Incorporated reviewer comments
0.9	2019-01-07	MW (UEDIN)	Editorial pass and Final draft submitted to EC
1.0	2019-01-31	MW (UEDIN)	Final version submitted to EC

Executive Summary

This standardisation report covers the standards-related activities for the PANORAMIX project. Activities such as interactions with IETF, W3C, and other standards bodies are reported. The standardisation strategy of PANORAMIX exists in order to create interoperabilty between multiple mix-nets. This involves the use of standards both in existing use-cases wherever possible, and then the standardisation of new mix-net specific components. The PANORAMIX project cannot guarantee the actual standardisation of the architecture, as standardisation is out of the hands of any EC-funded project. It involves the acceptance and processes of standards bodies whose decisions are outside of the control of the PANORAMIX consortium, but the relevant material was given to the IETF for review and possible standardisation. Note that this led to an invited presentation on the Sphinx message format at IETF 101 in London in April 2018 at the Security Area Advisory Group (SAAG) to an audience of hundreds of standardisation experts from across the world, leading to comments and support on PANORAMIX by non-European companies such as Cisco and Mozilla IETF representatives. Other standards bodies such as ETSI and ISO were also notified. In summary, the API was considered to be too high-level to be standardised, but there was interest in standardisation of the Sphinx mix network packet format at the IETF. The PANORAMIX project also participated in the creation of the Privacy Enhancements and Assessments Research Group (PEARG), a new effort that has led to the recognition by the IETF of the importance of privacy across all new Internet standards and provides a forum for the interaction of industry and academia over issues of privacy in all standards, including but not limited to standardisation of the Sphinx mix-network format, a crucial building block of the Panoramix mix-net. This work by PANORAMIX at the IETF has prepared the way for future standardisation of the Panoramix mix-net at the IETF after the lifetime of the project.

Contents

1. Introduction

This chapter states the purpose of the Standardisation Report produced at the end of the PANORAMIX project and its relationship to other project deliverables.

1.1 Purpose of document

This report captures the standardisation activities of the PANORAMIX project partners from September 2015 through to December 2018. Note that standardisation requires mature components and industry take-up, so the standardisation activities for the most part happened in 2018 as the research and deployment of the Panoramix mix networking implementation reached maturity, particularly the components described in D7.2.

1.2 Relation to other project deliverables

This document is a deliverable (D2.4) for Work Package 2 - "Dissemination" (WP2). This document covers the consortium's interaction with standardisation bodies. Standardisation, like dissemination, is applicable to all work packages (WPs) enabling the knowledge transfer from the consortium to the target audiences. This is especially important when considering the exploitation (Task 2.3) and standardisation activities (Task 2.2). In particular, D2.4 is related to the following WP2 deliverables:

- Deliverable #21: D2.2-Dissemination plan [KUL]
- Deliverable #22: D2.3-Dissemination Report I [KUL]
- 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. Use of Existing Standards

As per the mission of Task 2.2, existing standards have been used by the project wherever possible, including the usage of relevant IETF standards as outlined in the mixnet implementation developed in WP7.2 and WP7.3, as well as WP4. For encrypted e-mail, the IETF standards around SMTP were used for e-mail itself, as well as the standards for PGP developed by the IETF. The LEAP Encryption Access Project software deployed by Greenhost, rather than building new standards, simply made the infrastructure deployment of PGP and related IETF standards for improved authentication of e-mail, like DKIM and StartTLS.

Therefore, the usage of e-mail over the Panoramix mix-net will be compatible with popular e-mail clients (via *mailproxy*, see D7.3). The "Dmail" standards to be developed by the "Darkmail" initiative were never formed as an official part of the standardisation of next-generation e-mail at the IETF, although the work on K-9 mail (the mail client used for the mobile e-mail use-case in WP7) and Thunderbird (the primary mobile client used in the desktop LEAP-enabled use-case in WP7) also support the new grassroots Autocrypt[1] protocols for more usable key management for PGP-based e-mail. Greenhost and CCT are actively encouraging the standardisation of these new components as well. In terms of data collection by the partners, the data needed for the parameterization of the Panoramix mix-net project was produced using CSV but not released to the public due to its highly sensitive nature. Data collected by Greenhost from users in experiments for WP7 was done via an informed consent form, as per the General Data Protection Regulation, and with this data was collected via CSV and XML. In terms of the other use-cases of the Panoramix mix-network, relevant European and Greek e-voting standards were used by GRNET as detailed in WP5. Also, note for SAP that the W3C Customer Experience format was never officially standardised by the W3C and so was not used. Also, internally, SAP uses Linked Data and XML standards for its work in WP6. Therefore, all the use-cases of PANORAMIX tried to follow best practices in terms of deploying existing standards in order to increase uptake and maximise interoperability by using existing standards where appropriate.

[1] https://autocrypt.org

3. Choice of Standardisation Bodies

There has never been an attempt to standardise generic mix-nets before PANORAMIX, and thus there was not a clear pre-existing standards body where the outputs of the PANORAMIX project made the most sense. A liaison for the standardisation of the outputs of PANORAMIX was chosen in the second year of the project (Harry Halpin, formerly of the W3C and Advisory Board member of PANORAMIX) via Greenhost. A number of the new algorithms and protocols for mix-nets developed by the PANORAMIX project were considered relevant input for standardisation efforts and international, European, and national standardisation bodies like the IEFT, ISO JTC 1/SC 27 IT Security techniques, ETSI and the W3C. In particular, each of the aforementioned four standards bodies was contacted with relevant deliverables.

- **World Wide Web Consortium (W3C)** The general idea was that while the generic API could be applied both to messages that go over the Internet and those that work with special purpose-software that may not be exposed to the Internet, the parts of API that are adapted to Web-based (HTTPS) usage would make sense in the W3C. This enables the Panoramix API to go through individual-level royalty-free licensing agreement for the W3C, making it safer for other companies to use the underlying generic mix networking API. The W3C was contacted over the standardisation of the Panoramix API as given by WP4, as historically the W3C deals with APIs such as the WebCrypto and Web Authentication API. However, note that the W3C prefers to deal with APIs that directly impact web browsers, and so did not consider the Panoramix API, which is only used by PANORAMIX members at the current moment and not any web browsers or other large companies outside the PANORAMIX consortium, to be suitable for standards. Furthermore, due to the standardisation of W3C Encrypted Media Extensions (EME) by the W3C, there has been be considerable concern from both civil society and academia in pursuing standardisation at the W3C in general.

- **European Telecommunications Standards Institute (ETSI)** The Sphinx packet format was communicated to ETSI, who noted that it would be more suitable for the IETF.

- **International Standards Organisation (ISO)** Relevant publications including the new algorithms pioneered by WP2 and WP4 were sent to ISO JTC 1/SC 27 IT Security techniques in order to influence future ISO standardisation. However, after initial exploration of the various standardises bodies via the liaison, the work appears pre-mature for ISO standardisation.

- **Internet Engineering Task Force (IETF)**. The IETF standardises network-level protocols, such as TCP/IP and HTTP. The IETF has also historically been interested in security, such as TLS (Transport Layer Security). In the wake of the Snowden revelations, the IETF held the STRINT workshop (attended by Harry Halpin and George Danezis of UCL) with the W3C, where the IETF became explicitly interested in privacy.[1]

[1] https://www.w3.org/2014/strint/

Based on connections made at this workshop, the IETF expressed interest in the Sphinx network-level packet format.

Unsurprisingly, the IETF is more suitable for the network-level aspects of PANORAMIX. Given these results, the PANORAMIX partners decided to pursue the IETF as the most suitable standards body for future standardisation. The results of the engagement with the IETF throughout 2018 is described in the next section.

4. Standardisation at the IETF

The IETF has a straightforward process for standardisation. The steps are in the following order:

1. **Informational Draft**: A draft of a specification is written and submitted to the IETF.
2. **Bird of a Feather Meeting**: At an IETF meeting, an official meeting is held called a "Bird of a Feather" meeting (BOF). Prior to a Bird of a Feather meeting, interest can be engaged via existing per Area processes (note the IETF has multiple areas, such as the Applications Area and the Security Area). Note that a "Bird of the Feather" meeting can only happen once, and if there is not enough interest, the IETF can never continue standardisation in the area at a later date.
3. **Working Group Formation**: If the Internet Architecture Board (IAB) and Area Director believe there is enough interest in the Informational Draft and charter given by the BOF meeting, they will commence an IETF Working Group.
4. **Standardisation**: The Working Group creates a Draft RFC (Request for Comments) that eventually leads to the production of a Proposed Standard, which becomes an Internet Standard after approval by the IAB.

For the PANORAMIX project, the liaison Harry Halpin began a discussion with the Security Area Director, Eric Rescorla of Mozilla. Eric Rescorla took interest in the Sphinx packet format, although he noted that the API would be likely out of scope of the IETF. It was noted that the Sphinx packet format was not only being used by the PANORAMIX partners but also by a new blockchain company, Lighting Labs, that uses Sphinx as the default packet format for payment transfers linked to the Bitcoin blockchain. Thus, an **Informational Draft** was created from the specification for the Sphinx packet done as part of D7.2 (Section 7), entitled "The Sphinx Message Format" to be presented at the IETF meeting.[1] As the IETF was meeting in London near UCL researcher and inventor of the Sphinx message format George Danezis, the consortium approached Eric Rescorla to ask if it was time for a **Bird of a Feather Meeting**. Rescorla noted the high danger to future standardisation of mix-nets at the IETF if the Bird of a Feather meeting failed, as then Sphinx and mix-nets could never be standardised at the IETF.[2] Therefore, Rescorla suggested that the Sphinx Message Packet could be presented at the Security Area Advisory Group (SAAG) at the IETF. At IETF 101, Harry Halpin presented the Sphinx format (as George Danezis had teaching commitments at the time, and the IETF could not be flexible). The presentation was well-received, with over sixty standards experts from global companies attending. In particular, there was commentary on the future of standardisation of Sphinx by long-standing IETF representative of Cisco, Eliot Lear. The advice of Eric Rescorla was to build more support for Sphinx standardisation by helping with the creation a new Research Group focused on privacy at the IETF.

[1] https://katzenpost.mixnetworks.org/docs/specs/sphinx.html
[2] https://datatracker.ietf.org/meeting/101/materials/slides-101-saag-harry-halpin-sphinx-00

In addition to standards, the IETF maintains a parallel body, the Internet Research Task Force (IRTF),[3] for research that is of relevance to future standards at the IETF. This group, rather than maintain Working Groups for standards, maintains chartered Research Groups, such as the Human Rights Protocol Considerations (HRPC) Research Group. Harry Halpin convened with George Danezis a workshop with the NEXTLEAP EC Project[4] at University College London on Human Rights and Protocols on March 23rd 2018. This workshop brought together researchers from privacy, in particular from the PANORAMIX and NEXTLEAP projects, with civil society and industry representatives. Due to these discussions, more researchers in the field of privacy-enhanced technologies became interested in working with civil society and industry in standards. Therefore, after the London IETF meeting, there was a proposal to do a new research group into privacy, called Privacy Enhancements and Assessments Research Group.[5] The PANORAMIX Liaison held a meeting with civil society representative Shivan Sahib from Article 19 to help work through the participation and chartering of a new Research Group focused on a panel. With a broad charter focused on privacy-enhancing technologies and privacy reviews of existing protocols, the Privacy Enhancements and Assessments Research Group (PEARG) was officially proposed at IETF 103 in Bangkok, Thailand in November 2018 and we expect to be validated by IETF 104 in March 2019 in Prague. Note that the scope of PEARG is not limited to mix networking, but other proposals such as the new OTR ("Off the Record") version 4 have also been discussed. Currently, discussions about the future of the standardisation of the Sphinx network packet format will continue at PEARG until there is enough support for a Bird of the Feather Meeting at the IETF.

[3] https://irtf.org/
[4] https://nextleap.eu
[5] https://irtf.org/pearg

5. Future of IETF Standardisation

While PANORAMIX as a project is ending, its effects will continue through relevant standardisation processes at the IETF, and eventually other standards bodies as needed. We will continue to work with blockchain-related companies such as Lightning Labs at the next IETF meetings in order to get critical mass to continue the standardisation of the Sphinx packet format. Note that the route from an Informational Draft and the formation of a Working Group to full IETF standard typically takes from three to five years, so this work will continue after the lifetime of the PANORAMIX project. This work will happen in conjunction with the newly established Privacy Enhancements and Assessments Research Group. This Research Group plans to meet at every IETF meeting after 2018, providing a platform for the discussion and eventual standardisation of further mix-networking components such as the Panoramix API. Therefore, the suitable groundwork has been done to standardize the Panoramix mix-net after the ending of the PANORAMIX project itself.

Outside of the mix-net components, the PANORAMIX project is supporting the standardisation of authenticated encrypted PGP e-mail in a possible new PGP Working Group, building off the experience of Greenhost deploying the Panoramix mix-net and CCT with K-9 mail. For future secure messaging that builds on top of mix-networking, PANORAMIX will deploy the protocol under development by new Message Layer Security (MLS) Working Group.[1]

[1] https://datatracker.ietf.org/wg/mls/about/