Aggelos Kiayias—Ed. (UEDIN)
Merel Koning (Merel Koning Consultancy)
Thomas Zacharias (UEDIN)
Michal Zajac (TARTU)
Panos Louridas (GRNET)
Ania Piotrowska (UCL)
Benjamin Weggenmann (SAP)

System Abuse /Misuse and Mitigation Strategies (SUMMARY)

Summary of confidential Deliverable D1.5

March 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
0.9	2019-03-31	AK (UEDIN)	Summarised D1.5
1.0	2019-03-31	MW (UEDIN)	Final Pass

Summary of the Deliverable

Deliverable D1.5 is a consortium confidential deliverable which details misuse and abuse scenarios and provides techniques to be followed by partners and any other PANORAMIX operators to minimize any negative effects of such scenarios. The present document provides a summary of the deliverable content.

As a general perspective it is important to note that privacy is recognized as a fundamental human right, and at times is the only tool and last resort that law-abiding citizens have against oppression, censorship and abuses of power. As a consequence, privacy-preserving technologies exhibit a wide range of important law-abiding and rights-supporting uses. Nonetheless, privacy-preserving technologies are sometimes misrepresented due to recorded cases of providing a safe haven for individuals seeking to engage in criminal and generally illegal or abuse activity. This perception overlooks the fact that Internet's core design already allows for such individuals to have access to very sophisticated anonymisation or identity hiding mechanisms, e.g., through identity theft or by exploiting subverted computer systems (botnets) that scale at the order of many million nodes.

Given the above, the unavailability of privacy-preserving mechanisms at the core network layer disproportionately hurts legitimate users and restricts their needs and rights to privacy without depriving determined criminals from means to hide their activities. We emphatically argue that the benefits of a basic privacy-preserving communication mechanism such as PANORAMIX outweigh the disadvantages of its potential (criminal or non-criminal) misuse. On the one hand, the PANORAMIX codebase will be a facilitator for architecting privacy-by-design commercial and open source systems. On the other hand, it is expected that any misuse of PANORAMIX software will be small due to our choice of use-cases (and since perpetrators have access to effective anonymisation independently). In any case, abuses will be manageable through the technical, social, or, if necessary, even legal means available to system administrators, law enforcement agencies and court authorities (as numerous instances of successful law enforcement operations so far have indicated).

In the deliverable, we outline issues of misuse and abuse of PANORAMIX software on a technical level, covering all relevant specific attacks, as well as providing detailed mitigation strategies specific to each of our use cases. The deliverable concludes with a section that provides a legal perspective on PANORAMIX in the context of General Data Protection Regulation (GDPR) and more specifically Data Protection by Design and by Default (DPbD).

For the messaging use-case we refer to the email client and the Katzenpost system from WP7. The attacks against a messaging system deployed over PANORAMIX can be divided into two broad categories: (1) System attacks, that include Denial of Service (DOS), long-term disclosure attacks, impersonation attacks, dropping message attacks. (2) Content attacks that involve the distribution of any type of inappropriate content including threats, abusive messages, hate speech, spam etc. We describe the two classes as well as the available mitigations for providers.

For the e-voting use-case we divide our exposition in two parts. We first examine attacks and mitigations that are related to e-voting applications in general, followed by specific attacks and mitigations that pertain to the PANORAMIX framework. The attacks covered include double voting, vote theft, invalid vote recording and tallying, breaching the privacy and confidentiality

of the ballots, and voter coercion. Specific to the PANORAMIX framework issues include administrators, operators, or mixers themselves neglecting or compromising security by selecting inappropriate parameters as well as server administrators or intruders disregarding the common parameter configuration and deploy software with unsafe parameters. Another relevant threat is having non-experts take on the role of trustee or mixer and failing to set safe parameters, or being tricked into accepting insecure settings.

Regarding the privacy-preserving statistics use-case, which is the outcome of WP6, we focus on scenario specific attacks and mitigations for the taxi trip data which is the main application domain that the use-case focused on. The risks discussed include exploitation of communications metadata, eavesdropping, exposure of private information, spamming, corrupt mix-net operators, and fraudulent clients that attempt to corrupt the statistics calculations.

The final part of the deliverable consists of a study that was undertaken to discuss the relationship between the Panoramix tools and the concept of DPbD and the DPbD market. The study confirmed that the PANORAMIX project has succeeded in technically implementing the data protection principles in the developed tools. The PANORAMIX tools technically enforce a privacy-friendly manner of data processing in which the rights of freedoms of natural persons are respected. It is safe to say that the PANORAMIX tools implement the ideas of Data Protection by Design and by Default and that there is an emerging market for the deployment of such tools in Europe.