Initial release of the SafeCloud platform

D4.2

Project reference no. 653884

August 2017

Horizon 2020
European Union funding
for Research & Innovation

Document information

Scheduled delivery	31.08.2017
Actual delivery	31.08.2017
Version	1.1
Responsible Partner	CYBER

Dissemination level

Public

Revision history

Date	Editor	Status	Version	Changes
15.08.2017	K. Tarbe	Draft	0.1	Initial version
20.08.2017	F.Maia	Draft	0.2	INESC TEC review
27.08.2017	H. Mercier	Draft	0.3	UniNE Revision
29.08.2017	K. Tarbe	Draft	0.4	Incorporated the reviews
30.08.2017	K. Tarbe	Final	1.0	Finalise the document
31.08.2017	K. Tarbe	Final	1.1	Updated Figure 3

Contributors

K. Tarbe (CYBER)
V. Sokk (CYBER)

Internal reviewers

F. Maia (INESC TEC)
H. Mercier (UniNE)

Acknowledgements

This project is partially funded by the European Commission Horizon 2020 work programme under grant agreement no. 653884.

More information

Additional information and public deliverables of SafeCloud can be found at http://www.safecloud-project.eu

Table of contents

Executive summary

This deliverable summarizes the initial release of the SafeCloud platform on the SafeCloud website.

Introduction

The framework proposed by SafeCloud consists of three layers: secure communication, secure storage, and secure queries. Secure communication provides schemes for the establishment of channels amongst protocol participants employing technologies for tamper-resistant channels, ensuring confidentiality and availability. Secure storage provides techniques for reliable storage, such as long-term confidentiality, protection against file corruption or data deletion. Finally, secure queries provide cryptographic constructions from the database storage layer to the end-user processing requests. The overarching idea is to allow system developers to use the techniques provided by these three layers in order to achieve application-specific deployments. These deployments should surpass the state-of-the-art of existing tools with respect to functionality, performance and security. We recall Figure 1, from the general SafeCloud framework description.

Secure communication	State of the art: TLS secure channels	**Solution:**	**SC1 - Vulnerability-tolerant channels**	**SC2 - Protected channels**	**SC3 - Route-aware channels**
		Gives:	Tolerance to vulnerabilities in components	Decreased risk of fake certificates; resistance to port scans and enumeration of network infrastructure	Improved confidentiality with warnings about route hijacking and making harder access to communication
		API:	Extended secure socket API	Extended secure socket API	Extended secure socket API
		Provided by:	INESC-ID, TUM	INESC-ID, TUM	INESC-ID, TUM
Secure storage	State of the art: Encrypted storage	**Solution:**	**SS1 - Secure block storage**	**SS2 - Secure data archive**	**SS3 - Secure file system**
		Gives:	Block storage on individual data centers with fine control over data placement	Entangled immutable data storage for protection against tampering and censorship	Distributed secure file storage leveraging the secure block storage
		API:	Key/value	REST (S3 or similar)	POSIX-like
		Provided by:	UniNE, INESC TEC	UniNE, INESC TEC	UniNE, INESC-ID
Secure queries	State of the art: CryptDB	**Solution:**	**SQ1 - Secure database server**	**SQ2 - Secure multi-cloud database server**	**SQ3 - Secure multi-cloud application server**
		Gives:	Privacy of data against the server	Privacy of data against non-colluding servers	Privacy of data against non-colluding servers and clients
		API:	SQL	SQL	SQL
		Provided by:	INESC TEC	INESC TEC, Cyber	Cyber

Figure 1: Components of the SafeCloud architecture.

The SafeCloud platform is a set of solutions that are being developed in the SafeCloud project. The initial release contains the following solutions:

- Secure communications 1 – Vulnerability-tolerant channels – vtTLS
- Secure communications 2 – Protected channels – sKnock
- Secure communications 3 – Route-aware channels
- Secure storage 3 – Secure file system –SafeCloud FS
- Secure queries 1 – Secure database server
- Secure queries 3 – Secure multi-cloud application server – sharemind-SQL

The solutions are listed on the SafeCloud public website and are directly accessible at http://www.safecloud-project.eu/platform/. The landing page for SafeCloud platform mimics the SafeCloud architecture as can be seen on Figure 2.

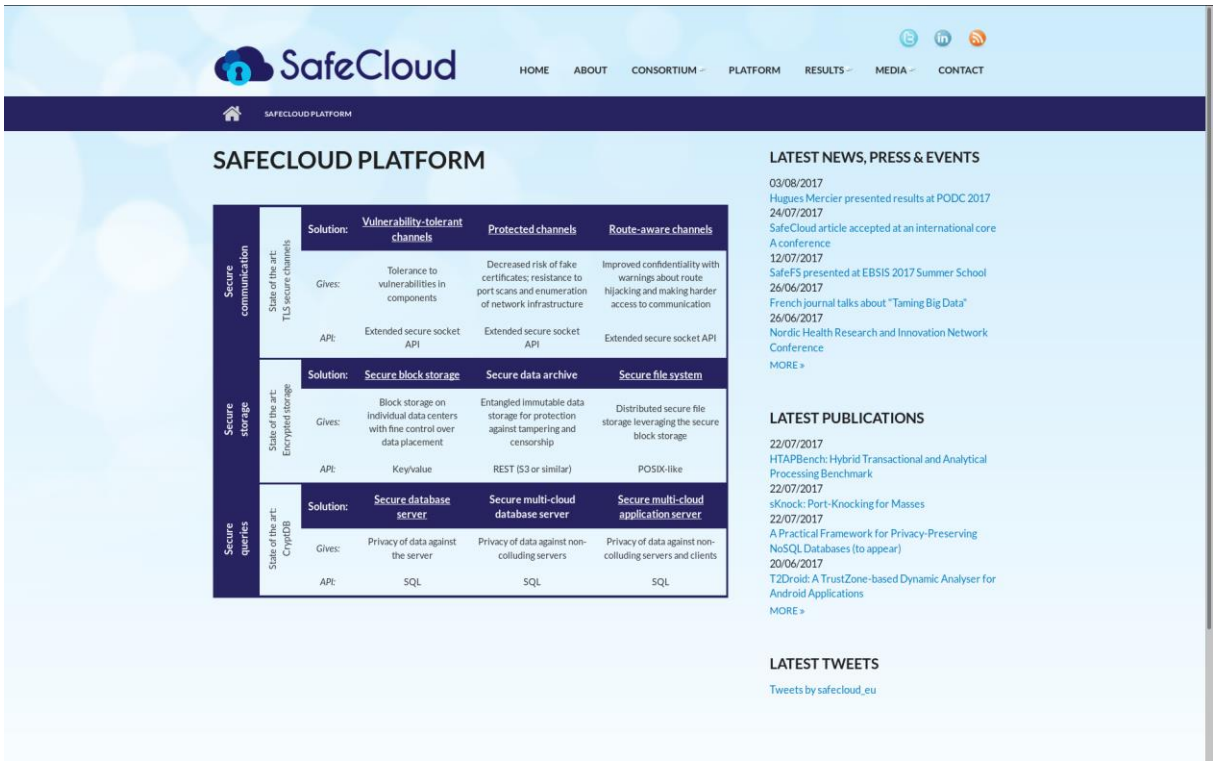

Figure 2: The landing page of SafeCloud platform on the SafeCloud website.

Content

The subpage for each solution contains information about where to obtain said solution, and instructions on how deploy it. Additional information like scientific publications and relevant public SafeCloud deliverables are also linked.

Detailed user guides are not available as part of the initial release, but the solution subpages will be updated and improved when such material is ready. For an example, the subpage for SafeCloud Secure queries layer solution 1 can be seen on Figure 3.

We favour Docker containers for distributing our software. Docker containers are easy to set up, test and deploy. These properties are paramount for the adoption of the SafeCloud technologies.

Figure 3: An example of a subpage describing one SafeCloud Platform component.