PhD Program in Computer Science and Mathematics
XXXIII cycle

Research Project

PhD Student: Ernesto Rosario *Russo*

Supervisor: Prof. Danilo *Caivano*
Co-Tutor: Dott. Felice *Vitulano*

Coordinator: Prof. Maria F. *Costabile*

PhD student signature _____

Supervisor signature _____

1. Research title: Cyber Security in Complex Systems.

2. Research area:

Software Engineering: Security Engineering.

3. Research motivation and objectives

The unstoppable process of digitization, interconnection and dematerialization in progress within management and production processes is progressively increasing the risk area and the area of potential cyber-attacks. Almost all the services provided today, both in the private and public sectors such as welfare services, are the result of interactions of complex systems understood as the set of organizational structures, processes, people, and infrastructures. The provision of these services is increasingly related to the cyberspace, i.e. a set of heterogeneous and interconnected networks, protocols and applications that surrounds us. Computer incidents that impact such infrastructures and services can have very significant economic consequences, at levels that range from national, company-wide up to that of individual citizens. Managing this growing risk requires an appropriate organizational approach, as well as processes and techniques, in consideration of the introduction of the European GDPR regulation (General Data Protection Regulation - EU Regulation 2016/679) which poses particular attention in identifying and protecting sensitive data order to protect sensitive information of European citizens.

The 2017 Clusit Report also highlights a worrying trend which, has recently seen a sustained growth in health attacks and attempts to steal data from public and private health facilities. Data that by nature are to be considered highly sensitive. Moreover, in this context a multiplicity of complex systems cooperate, and this makes everything even more critical by extending the perimeter of the possible attack.

It is therefore important to introduce an integrated approach to security management, which goes from the organization, understood as an organizational structure and ICT infrastructure to support complex systems, human resources and devices. There is also an urgent need to develop methodological and technological solutions that allow to collect, normalize and make all the information useful for the activities of "threat intelligence", or those activities that aim to extract information on emerging threats available.
This PhD research will focus on Cyber Security in Complex Systems, which will be analyzed along multiple dimensions: organizational, processes and tools.

An interesting route in this scenario seems to be that of the Blockchain. In fact in 2015, it was pointed out that it could be used in the IT for security management purposes and data storage and security. Thus, blockchain is definitely a valuable means for supporting the IT security, but we have to pay attention and address the new vulnerabilities that may affect the blockchain, such as "51%" and "Sybil" attack.

In this context, the goals of the research are

- **Goal 1**: Define organizational structures and ICT infrastructure with the purpose of addressing “security” from Software/Security Engineering point of view in the context of Complex Systems.

- **Goal 2**: Define threat intelligence processes and techniques with the purpose of use them for

addressing “security” from Software/Security Engineering point of view in the context of Complex Systems.

- **Goal 3**: Identify/define tools and techniques with the purpose of evaluating/use them for addressing “security” from Software/Security Engineering point of view in the context of Complex Systems.

4. State of the art

The problem of addressing security in complex systems is not new although it has recently become a critical need.

For example **Branagan at al. in [3]** assert that complex systems present a major challenge to risk analysis. Their tightly coupled components within complex systems conceal local threat sources that can be transmitted and magnified through the entire infrastructure, causing serious damage. Finding these threat sources is complicated both due to the system complexity and the barriers to sensitive security information data flows between autonomous managed systems.

There are also previous studies that deal with the more general problem of addressing security in enterprise architecture, and there are also well known approaches in this sense such as Enterprise Information Security Architectures (EISA), originally proposed by Gardner in a whitepaper titled “Incorporating Security into the Enterprise Architecture Process” published on 24 January 2006. It is a method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. A good review is presented in Oda et al [7] and also in [8] that addresses the problem from interoperability point of view.

The primary purpose of creating an enterprise information security architecture is to ensure that business strategy and IT security are aligned.

Further research is needed in order to be able to manage security in a cloud environment due to the revolution in the software architecture that it determined and the new concerns that this implied [9]. The same story was followed in the case of Software Service and Service Oriented Architecture [10].

Recently, there has been a strong interest around blockchain in the context of several industry applications, including critical infrastructures and complex systems, especially in the context of Health.

The first application that integrated the use of the blockchain was Bitcoin, which was proposed by **Nakamoto** in 2008[1]. He defined a purely peer-to-peer version of electronic cash “bitcoin” to allow online payments to be sent directly from one party to another without going through a financial institution. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

Shrier at al [2] discussed identity patterns guaranteed by blockchain technology, with many start-ups offering such solutions. Furthermore, it is highlighted that, as opposed to the classical methodology of securing systems that was deemed ineffective, the authors argue that with blockchain, a potential of “stack” eixts, rendering the cost of any breach or combination of breaches

much lower. Combined with strong encryption methods and zero knowledge proofs, it enhances the ability of data managers to protect critical information.
A step forward in the use of blockchain in complex system was done in 2015 when **Zyskind et al. [4]** has demonstrated that is possible to use blockchain protocols for permission management purposes. Indeed authors implemented a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. They implemented a trusted blind escrow service, storing encrypted data while logging pointers on the blockchain, so that transactions in our system are not strictly financial like original bitcoin definition, but they are used to carry instructions, such as storing, querying and sharing data.

Kosba at al [6] reports that existing systems have a lack of transactional privacy, as they are exposed on the blockchain. So they have presented a decentralized "smart contract" system that thus retains a transaction from the public view. The proposed solution can help programmers in writing smart contracts without having to implement cryptography, as it will be the compiler to handle aspects such as encryption, using cryptographic primitives such as zero-knowledge proofs.

The first definition of smart contract was provided by **Szabo[13]** in 1996, where smart contracts are "a set of promises, specified in digital form, including protocols within which the parties perform on these promises", and the first attempt to introduce a smart contract in blockchain was made by **ethereum [14**].

The Blockchain technology together with Smart Contract, as a storage and identity/permission management structure, can currently be used in the same way as an Enterprise Service Bus within complex service-oriented architecture.

It's also important to properly address the research problem concerning blockchain vulnerabilities, and evaluate these to appropriately design IT systems. **Bitcoin [12]** reports some vulnerabilities than can affect Blockchain-based application such as: Sybil attack, 51% Attack, Finney attack, Packet sniffing, Denial of Service (DoS) attacks, Forcing clock drift against a target node, and others. Many of these vulnerabilities are closely related to the blockchain and not to the specific bitcoin implementation.

When designing a software system, the regulations in force must be taken into account. All European enterprises are subject to the Regulation 2016/679 of the European Parliament and of the council also known as GDPR (General Data Protection Regulation) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The main topics discussed, are about: protection of privacy, cross-frontier data, data-processing law, access to information, data protection, and disclosure of information. Main principles that we will focus on are described in Art. 25 "Data protection by design and by default". Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user.

Hansen [5] emphasizes how the discussion on defaults should not promote that users lack necessary information and simply rely on the assumption that the best choice for them has been made already. This would not reduce, but rather increase the vulnerability of individuals' privacy.

5. Problem approach

Data privacy and security is a must in complex systems nowadays. The new legislation on the processing of personal data (GDPR) underlines that data protection must take place "by design" and "by default". It was decided to tackle the problem of defining a security model for complex

software systems, carefully analyzing aspects related to data protection by design and by default, at three distinct levels: Organizational, Process and Tools.

At an ***organizational level***, the objective is to define an organizational structure or function and a proper ICT infrastructure for addressing security. For example, the simple exposure of services becomes a point of vulnerability to attacks, so the more the number of integrations and endpoints is, the greater the number of potential attack points will be. Thus, the service providers need to adopt an organizational structure that include dedicated organizational units/functions for addressing the security problem. At the same time the infrastructure used for providing service need to be structured and organized in a safe way. An effective solution that face both aspect implies the use of security operations centers (or SOCs) and computer security incident response teams (or CSIRTs).
A security operations center (SOC), centralizes the roles responsible for protecting information security in the organization, and includes prevention; detection; incident management and response; reporting; governance, risk, and compliance; and anything to do with managing and defending information security within the organization. The goal of a SOC is to implement and oversee network, application, cloud, and user security, among other operational functions.
A CSIRT is a centralized function for information security incident management and response in an organization. It may roll up under a SOC, or it may act as the main security organization depending on your company's structure and security needs. It may also exist as a separate team in larger organizations. The ultimate goal of a CSIRT is to minimize and control the damage resulting from an incident, which is why so many different functions can be involved in some capacity.

An interesting point to study and address is how the use of Blockchain will impact on a SOC or on a CSIRT.

For what concerns the ***process level***, an important aspect to address is how software is designed and implemented for addressing data privacy and security.

In the design phase we must also take into account the appropriate choice of both the technological solutions and the communication and encryption protocols that are more likely to maintain a high level of security within the system. The common way of operating, on the other hand, involves software design based on functional and non-functional requirements, with little attention to safety aspects. At this stage Software Engineers have to be skilled in following certain programming techniques to prevent the emergence of vulnerabilities in the system. Organizations such as OWASP and SANS provide a ranking of the vulnerabilities that most impact on software applications and provide guidance on how to avoid programming errors that favor the emergence and the consecutive exploitation of the vulnerabilities.

Finally, with respect to the ***tools and techniques*** for supporting a safe development, there are tools for static analysis of software code that provide support in identifying possible weaknesses, which can be exploited to their advantage by attackers whether local or remote if not properly managed. Automated tools for static analysis, such as HPE Fortify, offer the advantage of being able to run on large code bases, but they also have the disadvantage of being able to execute only a set of rules that can look for defects inherent in general security. Therefore they can verify the existence of a potential vulnerability in the code, but cannot ascertain that the code is completely free of it. It is equally important to programmatically carry out analyzes of vulnerability assessment and penetration testing to reduce the chances of an attack causing damage to the system in terms of confidentiality, integrity, and availability.

6. Expected results

The result we hope to obtain is the definition and experimentation of a comprehensive security framework, based on the use of Blockchain Technology, for addressing security in complex systems at three major levels, organization, processes, tool and technique. The framework will be experimented in some relevant domain such as Health.
The reason is the number of data breach occurred in 2017 in this domain and the fact that here several complex systems cooperate in providing healthcare services to citizens. A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
The report of "Clusit" shows that on average 18 out of 20 health companies are affected by theft of health data. These violations involved 392 million records in 1931 incidents in 25 countries.
Blockchain is a promising technology to address security problem in healthcare, also if it is not enough mature to be used extensively. In particular the blockchain-based Electronic Health Record (EHR), in which the blockchain has the task of realizing the link between patient and healthcare provider, focus on the single components without putting itself in the optics of managing a complex system, without posing the objective of secure the whole system, leaving out the security management to the healthcare providers themselves.
Nowadays progress in the IT field allows physicians coming from different corners of the globe to collaborate in real time, while surgery is performed. Meanwhile, patients supported by the runaway technological development wear electronic monitoring devices, through which they can send continuous digital information to their health professionals about their health conditions. In this context, the development of new technologies in the healthcare sector and specifically the EHR systems must be related, going to favor aspects related to improving the efficiency and quality of the services offered both for health workers and for patients, making them participate in managing their health profile.
But the main points that need to be managed are the improvement of collaboration between various medical professionals who treat the same patient, and ensure the privacy and confidentiality of the patient are protected, and therefore manage the immutability of data concerning them. We believe that our research proposal can fill the lack just listed in the common EHR systems that can be found on the market, mainly focusing on the last but not least safety aspects.

Exprivia S.p.A. has among its subsidiaries Exprivia Healthcare IT s.r.l the potential both in terms of know-how and slices of the market to make commercial new EHR solutions such as that proposed in the research field.

7. Phases of the project

The research will cover a 3 years path and will be organized in the following phases (PH) and activities:

First year:

PH.1 Analysis of the needs

- Activity 1.1 Study of prior works in the literature on the security techniques of complex systems.

- Activity 1.2 Study of tools and procedures that in the real application case can help in solving the problem posed.

- Activity 1.3 Adaptation of the project proposal in relation to the real state of progress of Research and, at the same time, identify tools and solutions already available and useful for

translating the research results into industrial realities.

- Activity 1.4 Assessment of the real needs of potential users and identification of technologies among those analyzed that can meet these needs.

Second year:

PH.2 Proposition of innovation and Development of demonstrators

- Activity 2.1 Definition of methods and techniques for the evaluation of the proposed solutions.

- Activity 2.2 The innovations proposed in the previous point will be automated through demonstration prototypes to support innovation.

- Activity 2.3 This activity involves the integration of all the prototypes previously developed for the realization and subsequent experiments on the complex system.

PH.3 Design of the Empirical Research

- Activity 3.1 Design of the experiment aimed at qualitatively and quantitatively assessing the benefits produced by the use of the methods and techniques proposed by the approach.

- Activity 3.2 Definition of the measurement plan that will guide the collection and interpretation of experimental data.

- Activity 3.3 Identification and preparation of environments suitable for experimentation

Third year:

PH.4 Execution of the Empirical Research

- Activity 4.1 Execution of the experiment which involves the execution of planned experimental tests within the set up environment.

- Activity 4.2 Collection of experimental data according to the measurement plan defined.

PH.5 Result Analysis

- Activity 5.1 Analysis and interpretation of experimental data.

8. Result evaluation

The experimentation techniques used will vary according to the level of maturity of the defined framework and the experimental subjects identified.

Initially, an evaluation of the single framework components will be carried out by performing an in vitro experimentation. Once all the components will be integrated in a unique framework, a field experimentation (in-vivo) will be carried out in industrial environments. The experimentation will aim at assessing the level of security achievable thanks to the use of the proposed framework. For this aim a mix of assessment technique will be used::

- Vulnerability Assessment (VA) from within the network;
- Vulnerability Assessment (VA) from outside the network;
- Penetration Testing (PT).

The data collected resulting from the use of the proposed framework will be compared with those collected in other contexts where the proposed framework was previously not adopted. This will

allow us to compare and evaluate the improvement achieved. If a direct comparison between systems will not be achievable, it will be done by using literature data and statistics as well a post-mortem analysis.
An example of an indicator obtained after the vulnerability assessment may concern the number of vulnerabilities detected. It has a different value depending on whether the scan was carried out from within the network or from outside. An indicator that can be taken into consideration for the penetration testing phase concerns the percentage of successful attacks. Another indicator concerns the number of sensitive information stored or managed in "plaintext" inside and/or outside the network, this value is expected to be zero.
In this document only some of the quantitative specifications that are intended to be analyzed have been defined. These will however be extended and refined during the foreseen empirical investigations based on the case studies and projects that will be made available by the industrial component which in this project is very strong.

The proposed framework will be also investigated in a qualitative way in order to assess its sustainability and level of acceptance in industrial environment. This experimentation will involve Software Engineering and Industry manager from Exprivia SpA and other available Organizations. Moreover methods such as surveys and interviews will be adopted for this intent.

9. Possible reference persons external to the department

Prof. Macario Polo Usaola, Associate Professor, University of Castilla La Mancha, Spain

Prof. Corrado Aaron Visaggio, Associate University of Sannio

10. References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, (2008), https://bitcoin.org/bitcoin.pdf (Last access on January 9, 2018)
2. Shrier, D., Wu, W., Pentland, A.: "Blockchain & infrastructure (identity, data security)." MIT Connection Science (2016)
3. Branagan, M., Dawson, R., Longley, D.: Security Risk Analysis for Complex Systems. In: Information Security for South Africa (ISSA), pp. 1-12. (2006)
4. Zyskind, G., Nathan, O.: Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops (SPW), pp. 180-184. IEEE (2015)
5. Hansen, M.: Data protection by default in identity-related applications. In: IFIP Working Conference on Policies and Research in Identity Management, pp. 4-17. Springer (2013)
6. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Security and Privacy (SP), IEEE Symposium on (pp. 839-858). IEEE (2016)
7. Oda, S. M., Fu, H., Zhu, Y.: "Enterprise information security architecture a review of frameworks, methodology, and case studies" In 2nd IEEE International Conference on Computer Science and Information Technology. ICCSIT (2009)
8. Shariati, M,, Bahmani,F., Shams,F.: Enterprise information security, a review of architectures and frameworks from interoperability perspective. In Procedia Computer Science, Volume 3, Pages 537-543, (2011)
9. Bisong, A., Syed R.: An Overview of the Security Concerns in Enterprise Cloud Computing. In International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, (2011)

10. Coetzee, M.: Towards a Holistic Information Security Governance Framework for SOA. In Seventh International Conference on Availability Reliability and Security (ARES), pp. 155-160, (2012).
11. EUR-Lex Access to European Union law: Regulation (EU) 2016/679 of the European Parliament And Of The Council, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Last access on January 9, 2018)
12. Bitcoin: Weaknesses - Bitcoin Wiki, https://en.bitcoin.it/wiki/Weaknesses (Last access on January 9, 2018)
13. Szabo, N., "Smart Contracts: Building Blocks for Digital Markets", http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (Last access on January 16, 2018)
14. ethereum/wiki: A Next-Generation Smart Contract and Decentralized Application Platform, ethereum/wiki, https://github.com/ethereum/wiki/wiki/White-Paper (Last access on January 16, 2018)