Security Testing Reuse enhancing active cyber defence in Public Administration

Christian Catalano[1,2], Paolo Afrune[1,2], Mario Angelelli[1,3], Giovanni Maglio[2], Fabrizio Striani[1,3] and Franco Tommasi[1,3]

[1]*Department of Innovation Engineering, University of Salento, Lecce (IT)*
[2]*Cybersecurity Research Lab (CRlab), University of Salento*
[3]*Centre of Applied Mathematics and Physics for Innovation (CAMPI), University of Salento*

Abstract

The pervasive use of new technologies in sensitive contexts (e.g. management of critical infrastructures) is leading nation states to protect the cyber domain through the creation of governmental bodies with this specific responsibility. This requires the definition of specific protocols to manage different attack scenarios, rules, guidelines, and behaviors. Public administrations must follow such protocols to develop an appropriate cyber defence capability.

The aim of this paper is to introduce a new high-level framework to improve proactive cyber defence in the current Italian Public Administration. The general objective is to promote the reuse of information coming from security tests in order to optimise local resources while meeting global (national level) normative requirements and cybersecurity good practices. Protocols for different scenarios are described and expected micro-/macro-economic effects are discussed.

Keywords

Security management and governance, Proactive cyber defence, Security testing, Information reuse

1. Introduction

The use of ICTs in sensitive public contexts (e.g. public health care, management of power plants, *etc.*), in combination with private citizens' communication, is leading Public Organizations to consider compliance with law and defence against malicious cyber attacks as a matter of vital importance.

Due to the level of connectivity entailed by digital transformation, information management, which has always been an important but cross-sectoral factor related to specific domains, is now an asset with its own characteristics. In this framework we now refer to *cyberwarfare* [1, 2] as the use of ICTs to support military attacks against a country. We also mention the *fifth dimension of warfare*, which includes "information" among the domains to be protected, in addition to the classic ones (air, ground, space, and sea).

As a consequence, nation states are actively protecting this new domain through the creation of governmental bodies with such specific responsibility, defining specific protocols for given circumstances and attack scenarios, rules, guidelines [3, 4, 5, 6, 7], and behaviors [8] that Public

ITASEC – Italian Conference on CyberSecurity, April 7-9, 2021
mario.angelelli@unisalento.it (M. Angelelli)

Administrations must follow. In addition to internal rules defined by individual states for their own protection, members of the European Union also follow European regulations, such as NIS Dir. Ue n. 1148/16, Cybersecurity Act Reg. Ue n. 881/19, and Reg. UE n. 679/16, so called GDPR [9]. The defence of this new domain is neither simple nor straightforward, even following the recommendation of the nation states or the European Union: in fact, several factors contribute to the discrepancy between the rate of technological evolution and the adaptation time needed by public organizational structures or internal bodies.

In this contribution, we present a new proposal to improve proactive cyber defence in a specific scenario, that is the current Italian Public Administration (hereafter PA). This objective relies on operational and organisational adaption of processes in PA to already existing technologies, which motivates us in focusing on high-level, non-technical descriptions of the phases characterising proactive defence through security test reuse.

We start with a brief introduction to the current Italian context, highlighting the strengths as well as organizational challenges related to cyber defence in the PA. Then, we provide a description of our proposal, which aims at improving the resilience of the country system and developing an "active" (i.e. proactively defensive) cyber defence capability.

Specifically, we propose a variation of code reuse, namely, the reuse of results of Security Testing performed locally (e.g. Penetration Testing performed by local PA nodes present on the national territory) through a nation-level centralization. The main goal of this new framework is to enhance the protection of the most vulnerable links (local PAs) of a complex system (the National PA) while optimizing public resources.

2. Scenario Specification

2.1. Current situation in Italian PA

The context where the present proposal has been conceived is the current state of cybersecurity in Italian PA. Starting from the need to protect the Information domain, the notion of Information defence has been recently defined by the Italian law (2013, subsequently revised and adapted in 2017) with the aim of defining protocols to manage critical situations.

The current definition of the national cyber defence system involves several actors, among which the Prime Minister, the Interministerial Committee for the Security of the Republic (CISR), the Department of Information for Security (DIS), the External Information and Security Agency (AISE), and the Internal Information and Security Agency (AISI). More recently (2019) regulators have provided a clearer definition of national cyber security standards with regard to prevention and response to cyber events, with the aim of ensuring a high level of security of the networks, ICTs and IT services for PAs and public or private entities operating in the national territory.

2.2. Software development and Public Administrations

Beside the reaction to ongoing attacks, a fundamental approach to avoid damages in the Information domain is to *prevent* cyber attacks ("Prevention for Mitigation"). With regard to proactive defence, AgID defined the guidelines for the acquisition and reuse of software for

public administrations (May 9, 2019) with the aim of reducing costs of PAs. These guidelines require that the source code of the software produced by PAs (either on commission or through internal resources) be released as an open source project, so that other PAs can reuse the software. However, a PA node is not forced to use the software produced by other PAs. In fact, the guidelines describe the selection process in three steps [10]:

1. first phase: identification of needs;
2. second phase: analysis of the solutions available in the catalog of reusable code and open source solutions;
3. third phase: analysis of other solutions.

Each phase is preliminary and mandatory for the following ones. The third phase is divided into two sub-phases, where both the feasibility of the implementation of a new solution and the adoption of current proprietary ones are studied; the administrations are required to carry out both analyses, which will be compared during the choice phase ("make or buy" evaluation).

In particular, the solutions taken into consideration during the research phase must meet a series of constraints and criteria; in any case, if even one of the constraints is not met, the solution cannot be eligible. However, external constraints (time constraints, specificity of the issue raised by the PA node, *etc.*) may lead PAs to find and adopt proprietary software meeting all the constraints more likely than software-reusing solutions.

It is also stressed that proprietary software is often designed for a specific context, therefore its characteristics and configuration strongly depend on the laws and organization of the state (Italy in the present discussion). This also leads to consider such proprietary solutions as "niche products" since software produced for Italian PA is often not under the eye of the ethical hacker community and software houses rarely organize bug bounty programs[11].

2.3. Strengths and limitations of the current system

The development of national cybersecurity strategies has received interest because they have the potential to align the needs of national security with those of economic growth: the latter promote proactive security for the design of all digital policies. Indeed, proactive defence can increase the ability to prevent, deter, and detect cyber attacks response in a coordinated manner, including the different institutions involved in the cybersecurity framework.

There are different approaches regarding the countermeasures that a private company or a public body can adopt to prevent possible attacks to its infrastructures. Among them we mention:

1. Vulnerability assessment (VA) and Penetration testing (PT) [12, 13, 14]: the former allows to identify possible vulnerabilities within a network, while the latter consists in identifying and exploiting the vulnerabilities (already known ones and new *0day*s [15]) in order to take control of the system, as it happens in real attacks.
2. Static [16] and dynamic analysis of applications [17]: static analysis makes it possible to analyze a program without running it. This analysis can be done on the source code, or from the software executable (reverse engineering). Dynamic analysis consists in analyzing the software during its execution. Unlike static analysis, the result of dynamic analysis may depend on the input used.

3. Semi-automatic tools: these tools perform a check for known vulnerabilities. Then, the results are analyzed by a human eye [18].

While such approaches are well suited for anticipating possible consequences in the event of cyber attacks, in practice they present issues that cannot be ignored. Taking up some of the challenges presented in "The future of Cybersecurity in Italy: Strategic focus areas" white paper [8], we mention:

1. **Verification costs**: this is probably the most important aspect. In fact, not every company or entity can handle security costs, especially when the infrastructure to be protected frequently changes.
2. **Certifiability and verifiability of analysis**: they ensure that a vulnerability found during an analysis is reproducible, and then verifiable.
3. **Limits of automatic tools**: automated tools can only give an idea of what are the possible vulnerabilities in the assets under analysis. Specifically, some errors that arise from a human factor cannot be found automatically. In addition, some software makes automatic analysis difficult because of the adopted language: for example, interpreted languages, such as JavaScript, allows code injection.
4. **Vulnerabilities in specific IT environments and contexts**: this aspect is related to the previous one. Some vulnerabilities might emerge primarily as a result of the introduction of a given set of inputs. Therefore, the occurrence of vulnerabilities that are unlikely in a generic scenario might instead become more likely in specific application contexts. These vulnerabilities may therefore lead to a higher probability of intrusion and represent weaknesses for the entire ICT infrastructure.
5. **Environments for the security analysis of interoperable systems**: real testbeds for experimental analysis of third-party solutions, or solutions that come from untrusted sources.

3. Framework proposal

Based on the previous discussion, we introduce a proposal to promote proactive security and increase the ability to prevent, deter, and detect cyber attacks in a coordinated manner with the various institutions involved in order to meet some of the challenges highlighted in the White Paper.

The proposal consists in the high-level design of a new class of processes to manage information content regarding security tests as a resource. The expected effect of this design is to introduce a new observable criterion, i.e. the *useful information content regarding security test*, to formalise and enhance the concrete implementation of secure connections among nodes of the PA. This criterion not only can integrate the effective approaches and in-use recommendations with active cyber defence capability, but also represents an explicit discrimination among different nodes of the PA: the information content can be shared and accessed only based on the actual security needs of the different nodes of the PA, beyond their functionalities. In addition, our solution encompasses in a natural way the guidelines issued by AgID regarding code reuse for PAs: specifically, it solves several limitations of the current organization also highlighted in the White Paper, directly addressing the code reuse paradigm.

In order to clarify the points addressed by our proposal, we start from cost reduction for verification, which represents a major limitation for some institutions (such as small PAs). Then, software solutions adopted in distinct nodes with similar needs may take advantage from the reuse of security tests and the information on bug fixing: this can result in a larger set of in-use solutions to evaluate and update before moving to other proprietary software, which prompts cost reduction and enhances the adoption of certified and verified solutions. Finally, it is worth stressing that this approach could also solve the limitation introduced by automated tools, since the time saved in the analysis phase allows to transfer resources for additional, in-depth analyses. In this regard, multiple tests on software assets may be needed in order to explore vulnerabilities arising in different configuration settings: we stress that these tests do not represent redundancy, instead they improve the accuracy of PT/VA exploring potential vulnerabilities in different environments.

3.1. Details of the proposal

As well as for software, behind the concept of "reuse" there is the observation that different PAs acting in a common context often share the same solutions, either from AgID-promoted reuse or from proprietary solutions. As a consequence, in the case of VA/PT, the same components could be analyzed. The first implication is the violation of one of the main *desiderata* we want to satisfy, that is, cost minimization. An approach to solve this issue is to avoid redundant double-checks through the sharing of reports from VAs and/or PTs carried out by PAs. In particular, this allows to:

1. **minimize costs**: it is the obvious consequence of sharing. In this way, it is possible to analyze in detail only those solutions that are not yet equipped with security test results or with specific configurations;
2. **support small PAs in the protection of their assets**: shared results should be available to all PAs (limited to those concerned, for obvious security reasons). In this way, even PAs that are not capable of in-depth analysis can provide an appropriate level of security. At a deeper level of detail, the results could be accessible only to a given set of PA nodes, e.g. those nodes that have adopted the same software (nominal approach) or those that perform similar functions (functional approach);
3. **notifying new vulnerabilities**: the technical manager of a PA can be directly notified about new vulnerabilities in the assets he is in charge of. Furthermore, these communications can certify that updates have been notified, so the manager is required to update the system accordingly.

Given the sensitive context, results cannot be publicly shared and access must be granted only to certain specific entities. In addition, results should be made available without providing information about the PA that performed the test in order not to disclose its technological infrastructure. In any case, information can be shared only after the security bugs found have been fixed (case zero).

Operationally, this proposal requires both a dedicated platform, which establishes an official communication channel for notifications and information exchange encompassing the whole network, and an active participation of the technical staff in charge of its management. For

each PA node, the technical managers should be involved whether the PA receives a report after a security test, or after a modification of the assets. In detail:

1. The PA that has carried out the security test first verifies that the discovered vulnerabilities have been resolved by the vendor; then, the PA uploads the results on the platform specifying vendor, product, version, and impact of the vulnerability (CVSS score [19]) with a description of such vulnerability. It is also possible to indicate who carried out the test.
2. The PA that modifies its technological infrastructure, in terms of both hardware and software assets, updates these changes on the platform. In this way it can be notified for any already known problem, or for future ones.

Organisations such as CSIRTs are natural candidates to manage the platform, but the proposed framework introduces a bottom-up approach beyond the scope of CSIRTs: information and queries on security tests come from PA nodes and actively involve the whole PA network, including small PAs.

3.2. Diagrammatic representation of process schemes

The logical flow of interactions to enable Security Tests reuse is mainly determined by requirements. We start from the constraint coming from the current AgID guidelines and good practices in PT/VA.

- Security Test execution (e.g. PT) must be conducted by a third party vendor and must not be performed by the PA or the vendor that developed the software.
- There are standard scenarios that should be considered by any PA: information acquisition associated to new software introduced in the PA node; information retrieval and update regarding existing software in the PA node; information retrieval and update regarding new software in the PA node.
- there exists non-standard, context-based scenarios that may generate new process schemes. This eventuality has to be considered by default, in order to trace, assess, and possibly accept the process or correct it.

In order to contextualize the following process schemes in the same scenario while complying with the previous requirement regardless of the software being analyzed, we will adopt the convention of two distinct actors, associated respectively to software sales and to PT/VA services. Actors:

- PA (1, 2, 3, . . .): public administration;
- SW-1: Software vendor. This actor develops, customizes, and sells the software to PAs;
- PT-1: Security test vendor. This actor sells security tests to public administrations;
- PLATFORM: the platform.

3.2.1. Process scheme 1

1. PA1 buys software from SW-V1
2. SW-V1 provides the software to PA1 (e.g. `sw_calcoloImu v1.0`)
3. PA1 requires a security testing service from PT-V2
4. PT-V2 executes the security test and provides the report regarding security bugs and *0day* to PA1
5. PA1 sends the security bugs and 0days found during the security test to SW-V1 and requests the bug fixing of the software (e.g. `sw1_calcoloImu v1.0`)
6. SW-V1 executes bug fixing on the software according to the agreement between all parts (e.g. `sw_calcoloImu v1.0`)
7. SW-V1 releases the fixed version of the software (e.g. `sw1_calcoloImu v2.0`)
8. PA1 uploads on the platform the security bugs found during the security testing (e.g. security bug and/or *0day*) for software version 1 (e.g. `sw1_calcoloImu v1.0`) developed by SW-V1
9. PLATFORM notifies all PAs that have registered the software on the platform for vulnerabilities that have been added on the specific software version
10. Every single PA checks the software for which a vulnerability has been reported. At this point there are two possibilities:
    a) the PA has the vulnerable software
    b) the PA no longer has the software among its assets
11. PA2 requires the latest version of the software to SW-V1
12. SW-V1 releases to PA2 the latest version of software the (e.g. `sw1_calcoloImu v2.0`)

3.2.2. Process scheme 2

1. PA1 requires to PLATFORM an updated list of vulnerabilities regarding their software assets
2. PLATFORM provides the vulnerability list to PA1 for every single software owned by PA1
3. PA1 analyzes the vulnerability list from PLATFORM. The list can be made as follows:
    a) it contains recent information for some components owned by PA1
        i. PA1 contacts SW-V1 for bug fixing of information that meets 3.(a)
        ii. SW-V1 provides the fixed version
    b) it contains outdated information (e.g. the date of the last security test performed on a single software version is older than 6 months) or does not contain information (e.g. some security test has never been performed on that specific software version) for some components owned by PA1
        i. PA1 requires a security test to PT-V2 regarding the assets that satisfy point 3.(b)
        ii. PT-V2 executes the security test and provides the report regarding security bugs and *0day* to PA1
        iii. PA1 updates its assets based on the report provided by PT-V2
        iv. PA1 uploads the results of the security test on PLATFORM

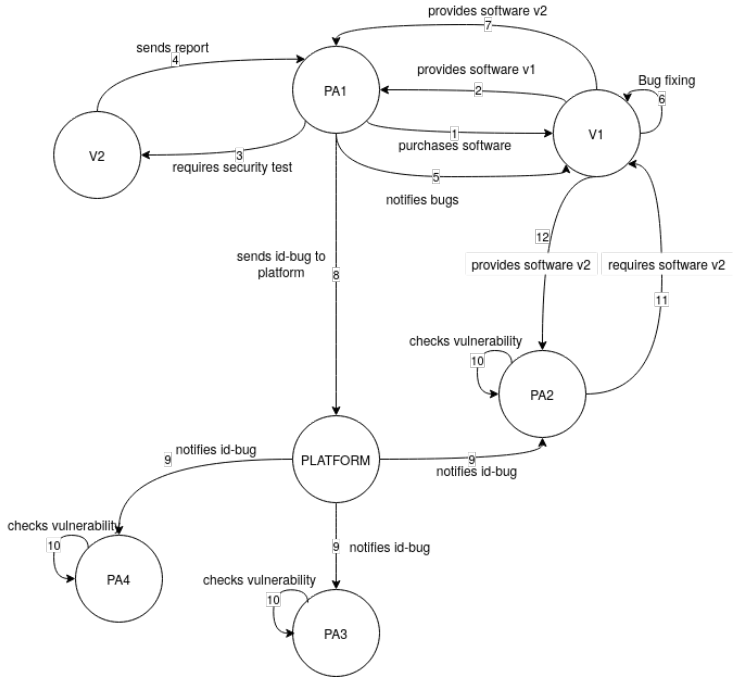

Figure 1: Process scheme 1

Note that the attributes “recent information” and “outdated information” in Point 3 of Process scheme 2 are related to implementation aspects that are independent of the proposed logical structure. That is, the attributes may depend on factors such as the addition of new functionalities to the software under consideration, individual assessments by the PA, or criteria related to the periodicity of testing based on safe software management guidelines (e.g., “to be performed preferably every 6 months”).

3.2.3. Process scheme 3

1. PA1 buys new software assets from SW-V1
2. SW-V1 provides the assets to PA1
3. PA1 updates its inventory by adding newly acquired assets
4. PA1 adds newly acquired assets to PLATFORM
5. PLATFORM provides a list of known vulnerabilities regarding the latest assets added based on the information provided to the platform
6. PA1 analyzes the report to check that all new assets are up-to-date and have no known vulnerabilities

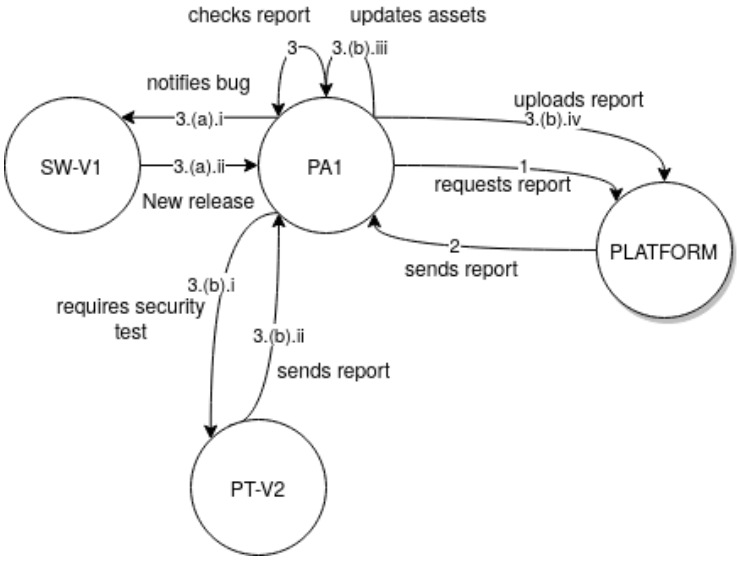

Figure 2: Process scheme 2

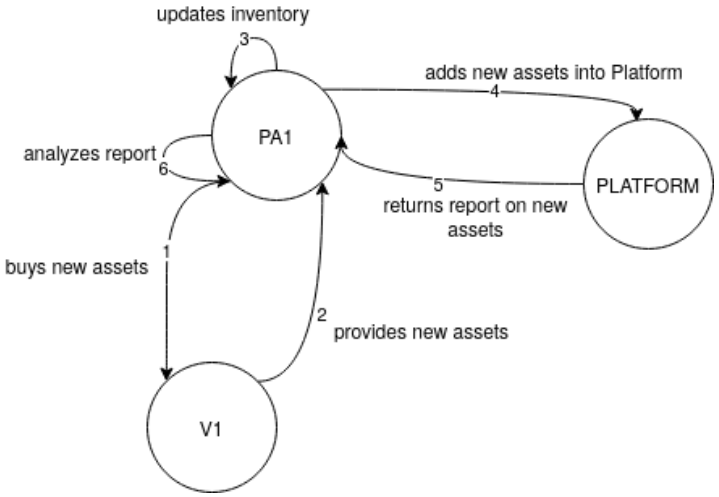

Figure 3: Process scheme 3

4. Expected measurable economic effects

The implementation of the reuse of results of PTs described above could bring effective advantages both from a microeconomic and a macroeconomic point of view. These advantages represent a tangible, i.e. measurable effects, since the economic indicators can be assessed to evaluate the effectiveness of the proposed approach at different scales:

- improved evaluation of public spending policies: if the description of some vulnerabilities has emerged during the execution of a PT and the information regarding the patched

version of the same software under test is available, public spending can be reallocated on different investments;

- competitive advantage for territorial ecosystems: the whole country system would gain competitive advantage, for example through the empowerment of PAs that are unable to execute PT in a regular and constant manner due to budget issues or difficulties in finding specialized personnel;
- support to policy makers in the spending review, based on secure information from a trusted network;
- choice of the different sectors where to intervene: saving in a sector enables potential reinvestments in other ones (e.g. cultural goods, environment, health, *etc.*).

We can identify some advantages from the microeconomic point of view using the concept of *economies of scope*: with this term we refer to the savings resulting from the joint production of different products, or the pursuit of different objectives through the use of the same production factors. In this way, one can reach the production of different types of goods with the same class of resources. Using this notion, it is easy to identify the effects of the reuse of PTs results as the benefits of the investments made by an individual entity of the PA for all the other entities sharing the same need.

On the other hand, the proposal would also have a macroeconomic effect due to the considerable savings by the PA. In order to quantify them, we start from the public savings in formula $S_{pubb} = T - G$: a lowering of the public expenditure (G) would mean greater public savings, which could allow a lowering of taxes (T). It is also worth recalling that overall savings are given by $S = S_{priv} + S_{pubb}$. Therefore, greater public savings would lead to greater overall savings. In the Keynesian theory, the macroeconomic identity $S = I$ applies. Then it is evident that the increment of the overall savings corresponds to increased investment (I) and, therefore, prompts an overall improvement in national GDP.

Macroeconomic advantage emerges not only from greater economic-financial resources that may cover different needs, but also in terms of redefinition of strategies shared among different local nodes of the PA. A modification of the structure of information sharing entails a corresponding change in the set of feasible solutions or policies for resource allocation; in particular, the present approach does not exclude possible strategies, but it introduces new ones. A practical example is the reuse of useful information from VA/PT carried out on some specific components of a given asset: if a PA node does not have sufficient resources to ensure the fulfillment of all the criteria required by national guidelines, it can limit to recover missing information, assuming that complementary information is already available after testing and sharing actions by other nodes. In principle, this knowledge can support the strategic administrative planning of individual nodes, bringing possible reciprocal benefits.

Finally, the reuse of security tests or, more precisely, of the useful information they provide, can also lead to advantages at supranational, e.g. European level. This aspect concerns the adherence of the policies adopted by the EU with regard to open data. Moreover, the reuse of information coming from security tests can be configured as a secure-by-design channel of communication between two types of actors, namely, the purely national level (PA) and the international level (vendors).

5. Conclusions and future work

This contribution proposes a new framework that aims at supporting national PA in meeting the requirements posed by digital transformation in compliance with European recommendations. In turn, this framework also paves the way for new savings and business opportunities for public and private Organizations.

There are several research directions to refine this proposal: first, information coming from the reuse of security tests assumes new value, which can become a new asset for Organizations. The added value brought by information sharing can be exploited to explore new organization reward models with the goal of enhancing transparency in PA-oriented cybersecurity. Such a perspective is set up as a form of *circular economy with immaterial resources*, which is strategically important not only for individual PA nodes, but also for the country system and, more generally, for the EU. Also Vendors could get benefits from such an framework: increased transparency in the security testing requirements for a specific node of the network may integrate partial information already available to the PAs, both in terms of reduction of fallacies in the testing process (for instance, violations of the condition in the Guidelines) and market access beyond the local scale (i.e. countrywide).

In this work we have presented a high-level structure without providing a specific real-case context: this approach is motivated by the possibilities offered by this level of abstraction, since the proposed scheme may be adapted to several distinct contexts. There may be situations where different security needs and conflicting requirements (e.g. confidentiality vs. accessibility) lead to *ad hoc* implementations of this framework. For instance, new security layers may be introduced, where different offices or Entities within the stratified PA structure have their own security requirements and associated counteractions. The opportunity to adapt the logical structure to the contextual characteristics of nodes fits well with the complexity of Italian PA and may enhance secure information sharing between central and local/periferic levels. On the other hand, the context-dependent implementation of the present framework, which is typical of large-scale technological systems, requires specific validation procedures for each context.

In this way, the proposed framework:

- introduces data separation in the access to information, making information exchange asymmetric between these layers as formally defined by the Principle of Least Privilege [20]: local layers cannot access to central information preventing vertical privilege escalation access;
- may support the definition of communication layers (e.g. alerts) based on specific security qualification levels that are expected or required at each node. This enhancement may stimulate a clearer definition of fields of competence and responsibilities related to cybersecurity in the PA, in order to send relevant information to target Entities that are able to interpret it and counteract cyber-risks;
- allows to share information without getting access to the original data (e.g. original reports), which may be confidential. We can get the access to information without disclosure providing only confirmation for specific queries by a node of the PA regarding its software assets, which promote the required counteractions and enhance, rather than compromise, the security of the PA network.

References

[1] J. Carr, Inside cyber warfare: Mapping the cyber underworld, O'Reilly Media, Inc., 2012.

[2] V. A. Almeida, D. Doneda, J. de Souza Abreu, Cyberwarfare and digital governance, IEEE Internet Computing 21 (2017) 68–71.

[3] AgID, Linee guida di sicurezza nello sviluppo delle applicazioni, https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lineeguidasicurezza-introduzione.pdf, 2017.

[4] AgID, Linee guida per l'adozione di un ciclo di sviluppo di software sicuro, https://www.agid.gov.it/sites/default/files/repository_files/allegato_1-_linee_guida_per_ladozione_di_un_ciclo_di_sviluppo_di_software_sicuro.pdf, 2020.

[5] AgID, Linee guida per lo sviluppo sicuro, https://www.agid.gov.it/sites/default/files/repository_files/allegato_2_-_linee_guida_per_lo_sviluppo_sicuro_di_codice.pdf, 2020.

[6] AgID, Linee guida per la configurazione per adeguare la sicurezza del software di base, https://www.agid.gov.it/sites/default/files/repository_files/allegato_3_-_linee_guida_per_la_configurazione_per_adeguare_la_sicurezza_del_software_di_base.pdf, 2020.

[7] AgID, Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design, https://www.agid.gov.it/sites/default/files/repository_files/allegato_4_-_linee_guida_per_la_modellazione_delle_minacce-dlt.pdf, 2020.

[8] R. Baldoni, R. De Nicola, P. Prinetto, Il futuro della cybersecurity in italia: Ambiti progettuali strategici progetti e azioni per difendere al meglio il paese dagli attacchi informatici, Laboratorio Nazionale di Cybersecurity (CINI)-Consorzio Interuniversitario Nazionale per l'Informatica (2018).

[9] P. Voigt, A. Von dem Bussche, The eu general data protection regulation (gdpr), A Practical Guide, 1st Ed., Cham: Springer International Publishing 10 (2017) 3152676.

[10] AgID, Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni, https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf, 2019.

[11] A. Kuehn, M. Mueller, Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities, in: 2014 TPRC Conference Paper, 2014.

[12] J. N. Goel, B. M. Mehtre, Vulnerability assessment & penetration testing as a cyber defence technology, Procedia Computer Science 57 (2015) 710–715.

[13] I. Yaqoob, S. A. Hussain, S. Mamoon, N. Naseer, J. Akram, A. ur Rehman, Penetration testing and vulnerability assessment, Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org 7 (2017).

[14] P. S. Shinde, S. B. Ardhapurkar, Cyber security analysis using vulnerability assessment and penetration testing, in: 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), 2016, pp. 1–5. doi:10.1109/STARTUP.2016.7583912.

[15] M. A. McQueen, T. A. McQueen, W. F. Boyer, M. R. Chaffin, Empirical estimates and observations of 0day vulnerabilities, in: 2009 42nd Hawaii International Conference on System Sciences, IEEE, 2009, pp. 1–12.

[16] P. Ferrara, F. Spoto, Static analysis for gdpr compliance., in: ITASEC, 2018.

[17] T. Ball, The concept of dynamic analysis, in: Software Engineering—ESEC/FSE'99, Springer, 1999, pp. 216–234.

[18] Y. Stefinko, A. Piskozub, R. Banakh, misc and automated penetration testing. benefits and drawbacks. modern tendency, in: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), IEEE, 2016, pp. 488–491.

[19] P. Mell, K. Scarfone, S. Romanosky, A complete guide to the common vulnerability scoring system version 2.0, in: Published by FIRST-forum of incident response and security teams, volume 1, 2007, p. 23.

[20] F. B. Schneider, Least privilege and more, in: Monographs in Computer Science, Springer-Verlag, 2003, pp. 253–258. URL: https://doi.org/10.1007%2F0-387-21821-1_38. doi:10.1007/0-387-21821-1_38.