Proceedings of the Federated Conference on Computer Science and Information Systems pp. 547–554
DOI: 10.15439/2019F261
ISSN 2300-5963 ACSIS, Vol. 18

Information Systems Development and Usage with Consideration of Privacy and Cyber Security Aspects

Janusz Jabłoński
Uniwersytet Zielonogórski
ul. prof. Z. Szafrana 4a
65-516 Zielona Góra, Poland
Email: j.jablonski@wmie.uz.zgora.pl

Silva Robak
Uniwersytet Zielonogórski
ul. prof. Z. Szafrana 4a
65-516 Zielona Góra, Poland
Email: s.robak@wmie.uz.zgora.pl

***Abstract*—One of the contemporary problems, and at the same time a challenge, with development und usage of supply chain Information Systems are the issues associated with privacy and cyber security, which emerged due to new requirements of legal regulations and directives. The human factor belongs to the biggest risks within these issues. Leak of information, phishing, unauthorized access are the main problems. Also vulnerability of the systems due to new information technologies is an important topic. In this paper we discuss development and usage of Information Systems with regard to the security aspects associated to the software development lifecycle. We present our approach on examples of a user authentication process in logistics.**

I. Introduction

THE information security and cyber security are strongly associated with the technological infrastructure of computer networks and computer systems processing information. A computer system is secure if the user can relay on its functionality and the installed application software is working consequently the specifications. Developing software applications with compliance to the user requirements is not sufficient, because the developed systems should additionally be secure and consistent with the current state of law regulations.

In this paper we will approach a problem of the exchange of a vast amounts of data in supply chains with respect to the data privacy and security issues. There is the European Union's General Data Protective Directive GDPR concerning the protection of natural person with regard to the processing of personal data [1]. On the background of this regulation and of the Payment Services Directive 2 PSD2 [2], which are concerning transaction systems on financial markets, and Fintech [3], the development of the secure software business applications turns out into a great challenge. In our paper we will suggest some improvements to the IS's development process, which result from the above stated system requirements and the further implications regarding privacy and data security aspects.

The supply chain defines the network that comprehends all the organizations and activities associated with the flow and transformation of goods from the raw material stage, through to the end user, as well as the associated information flow [4]. In our paper we will concentrate on threats and possible solutions demanded for the secure supply chain activities and flow of information.

In the inter-organizational information systems, which link the companies to their suppliers, distributors and customers, a movement of information through electronic links takes place across organizational boundaries, between separately owned organizations. It requires not only the electronic linkage in form of basic electronic data interchange systems (as for purchase orders), but also the interactions in complex cash applications and information systems or an access to shared technical databases. Thus, the problems associated with the privacy and security are also very viable in supply chains contexts.

The credibility of information as also especially the trustworthiness of the participants in supply chains is required. In transportation and logistics, in order to eliminate a possibility of the documents frauds, non-existent suppliers or recipients, an essential element of the risk elimination in supply chains is the credibility ensured by an authentication.

We believe, that the enterprise information systems being a part in a logistic supply chains should be secured during all stages of their life-cycle, and will give some guidelines for development-time und run-time of the IS.

The security concerns become additionally significant with the regulations like General Data Protection Regulation (GDPR) in the European Union and other regulations to be expected coming soon. The problem is that they use terms like "reasonable security procedures" or "appropriate practices" and do not advice what type of technology is needed to protect the personal and enterprise data. They only state generally about the responsibility of the organizations to keep data secure [5].

Therefore, as stated previously, in our paper we will analyze how to integrate the needed privacy and (cyber) security aspects into the life cycle of Information systems to

ensure the above mentioned secure procedures and appropriate practices. For this aim the rest of the paper is organized as follows.

In Section 2 we will characterize the main threats and vulnerability aspects considering the information systems security due to the usage of new emerging IT solutions and the influence of EU regulations associated with privacy and security concerns. In Section 3 we will review some aspects of cyber security and then propose some solutions applicable for developing and using information systems. The aspects of information security due to the problems with user authentication and data access control are the main topics in Section 4. In Section 5 we give some examples for conducting user authentication and show how they can support an achievement of the required privacy needs for IS of enterprises according to the EU regulations. In the last Section we conclude our work.

II. VULNERABILITY OF INFORMATION SYSTEMS SECURITY DUE TO NEW TECHNOLOGIES

The numerous cyber attacks associated with, i.e. a stealing of the identity, the leaks of vulnerable data, or the frauds in billion of dollars yearly raised new approaches in the risk taxing, as for instance shown by Global Economic Crime an Fraud Survey for 2018 in [6]. The rethinking of the ways and approaches for development and usage of software systems and considering the proper handling of modern technologies, and also the computer networks security problems are needed. In addition, the raising numbers of mobile technology users of Smartphones and tablets with the integrated Wi-Fi equipment, and the widening popularity of operation systems like Android and iOS, caused that the mobile systems are replacing gradually the traditional computer systems.

In [7] there is a diagram depicting the percentage of the mobile OS used on market based on the report showing the growing dominance of the mobile operating systems in the last two years. The mobile devices are currently used for the e-mail checking, news viewing, the communication in social networks, and also for the payments. Operating in such environments often requires a usage and sending of vulnerable private data, such as private contact data or/and the bank account information directly with the mobile devices. It could happen that a user do not have the sufficient consciousness and knowledge of the threats caused by the neglecting of the security features on the stage of software application development.

Considering the human factor, there could be also the security risks connected with the intended conscious handling of some enterprises or programmers developing software applications, which are acting in contradiction with the users aims and also the laws regulations with the aim of processing and steeling of vulnerable user data. Examples of such behavior are known, and widely described in the Internet and include the deeds such as notorious hacker groups, the hybrid warfare [8, 9, 10], up to the cyber troops [10, 11].

We believe that activities aimed at eliminating of vulnerabilities related with the human factor could be the particularly the forecasting of the attacks, such as attack vector [12] (i.e. email attachments, pop-up windows, deception, chat rooms, viruses and instant messages) and also regarding them possibly early already on the stage of developing software and the by usage and maintenance of IS. Such actions will be needed not only for new systems (developed from scratch), but also in maintaining already existing relative new modern and legacy systems.

Moreover, considering the vulnerabilities enumerated by the Open Web Application Security Project OWASP Foundation [13], the counteractions, or possibly elimination of the some threats is also strongly desirable by defining constrains for systems, which are using new technologies like cloud computing [14] and/or blockchain [15].

By developing software systems there will be some additional basic considerations viable for aims of their future security. To begin with gathering of user requirements and enhancing them with the law regulations related to the user privacy and data security aspects. A proper choice of the software architecture of a software system, which will be supporting the required security needs, and also the secure procedures for user authentication and system access control are recommended. There are also some additional aspects in the development phase, as for instance the usage of libraries, which are resistant to the buffer overflow, eliminating of the redundancy by avoiding linkage to the external resources, and also eliminating redundancy in computer network communication between the hosts, etc. We will consider these requirements in the following Sections.

III. CYBER SECURITY SOLUTIONS

While the ERP systems with the embedded automated financial settlements are the constituents of supply chains, their authentication process should accomplished at a proper security level. For this reason to stay in accordance with formal requirements, the systems in logistics and supply chains should meet the requirements of the dynamic authentication in order to eliminate a possibility of hijacking or the replay attack as in case of a spoofing attack.

The authentication and access control to digital resources are the crucial elements for ensuring security in a cyberspace. The EU Regulation 2015/1502 from 8th of September 2015 defines the minimal technical specifications and the procedures for the assurance levels of electronic identification and trust services for electronic transactions at the internal Europe Union market. The regulation defines tree assurance levels [16] as:

- Low,
- Substantial, and
- High.

They should be applied for electronic identification means issued under an electronic identification scheme. Additionally in the regulation the "dynamic authentication" is defined with the meaning of "an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity".

According to this regulation for the substantial and high assurance levels in authentication mechanism, the sending of person identification data should be preceded by a reliable verification method by the electronic identification means, and its validity assured by a dynamic authentication.

For this electronic proof it is also required to be modified (to alter) with each new user authentication, as well as to be resistant to the attempts of off-line analysis.

For meeting of the above requirements included in the EU regulation, concerning the dynamic authentication mechanisms, we believe that a promising solution may be the usage of cryptography with one-time passwords or one-time key, referred to as OTP [12]. A proof for semantic security of crypto-systems constructed with regard to the rule for one-time key in cryptography was given in year 1949 by C. Schannon in [17]. Nevertheless, the research efforts regarding secure cryptographic systems implementing the OTP rules are still ongoing.

We should emphasize the fact that the systems, which implement the OTP rule are potentially resistant to the cryptanalysis with the quantum computers. Cryptography considered as resistant to the attacks by usage of quantum computing is referred as post-quantum cryptography [18].

The transaction security is also required in Fintech services, such as e-banking, e-health, etc., where the keeping anonymity and also the user authentication should be in accordance with the high assurance level. At the same time the dynamic authentication on the middle and high assurance levels, as for data which is secret and with all right reserved, is defined by the Payment Service Directive (EU) PSD2.

It is to emphasize that the above mentioned GDPR and PSD2 have been indeed introduced as regulations, but until now, the applications implementing the dynamic authentication systems conforming to these requirements are lacking.

There are some known approaches to a deal with the above problem of a secure authentication, like a research on the one-time keys in user authentication method RUBLON [19]. In the RUBLON system based on a solution given in the patent [20] is applied, and it conforms to the OTP and semantic security requirements. What is more, on the base of the solution included in the patent [20] the enterprise DCD has applied this solution in the project CryptONE (unconditional secure crypto-processor [21]), where the decryption takes place with one-time passwords.

The concept of Industry 4.0 [22] has shown some digital trends, such as the process automation and usage of the artificial intelligence in the decision processes. Therefore, in the future the authentication not only of the persons and entities, but also of the devices and the processes will be needed.

Regarding the trust, privacy and security aspects in the life-cycle of information systems with respect to the threats and vulnerabilities discussed in Section 2, below we summarize and suggest some guidelines for development and system usage (run-time) in the IS lifecycle.

In the development and implementation stages of the lifecycle, beginning with the system analysis phase, the obtained user requirements should be complemented with the requirements resulting from the law regulations concerning privacy and security. It especially applies to of data to be exchanged by Information systems in Supply Chain Management SCM in cloud environments as presented in [23]. Thus, the new technologies like cloud computing are offering potentially more secure data storage based on duplication and distribution [24].

In the system development and implementation stages there are some additional important issues to be regarded as crucial for more reliable protection of privacy and security aspects of software systems, such as:

- A deliberate choice of a system architecture,
- A secure (user) authentication procedure and data access control,
- A choice of the appropriate libraries according to the security requirements,
- The strict rules for the usage of external sources,
- The following the network security rules and the usage of appropriate computer network protocols,
- The proper packet management in mobile devices.

The first issue is a decision for a choice of the system architecture, like centralized, (or decentralized) or Cloud Computing usage, and it is dependent on the kind of a developed application, i.e. the usage of further technologies such as blockchain. The expansion of the systems based on new cloud technologies and cloud computing [25] by using services as IaaS – Infrastructure as the System, PaaS - Platform as a service, SaaS – System as a service, as also the growing usage of mobile devices set additional requirements on implementing solutions for an access to the remote data resources. It is particularly important to regard whether the system is processing personal data, according to the EU GDPR rules, or it is a transaction system – in accordance with the PSD2 directive. In such cases the additional considerations to cyber security are desirable and needed.

In case of the Client/Server n-tier architectures the sensitive personal data should reside on a back-end data server without a direct Internet access.

The second issue – the process of authentication procedure and data access control should be conducted in accordance with the requirements of PSD2 Directive. Therefore, we suggest to consider the two-factor authentication 2FA, with the cryptographic strong second factor. We can also recommend a usage of an authentication method based on Challenge-Response, as proposed in OCRA specification [26]. Moreover, the usage of one-time keys OTP is recommended, as mentioned in the previous Section. This way of usage of OCRA and OTP is simple to implement and will increase the security of the (user) authentication process.

The third implementation issue is a deliberate choice of appropriate libraries according to the security requirements. The libraries resistant to buffer overflow and the adequate programming methods for strict control of data types are recommended, as described in [12].

The next issue is a deliberate usage of external sources. The rules for conscious usage of external sources, especially for mobile applications should include the possible restrictions of a necessary usage of the external resources and libraries [28].

The network security rules and usage of appropriate computer network protocols should be carried out according to the principles indicated by W. Stallings and L. Brown in [12].

The last issue, is a proper packet management for mobile devices. A developed software should prefer the usage of packages that are resident on the device, i.e. not dynamically loaded during their usage at the run-time.

At the running (operational) phase, we also emphasize one more time the crucial role of a secure user authentication and the usage of dynamically changing one-time keys. These issues will be considered in the next two Sections.

IV. AUTHENTICATION METHODS

From the perspective of the enterprises the problems with data protection in business processes can be seen from the different perspectives, as described in [23] and [24]. The one perspective is considering the security and privacy of sensitive business data which belongs to the enterprise or its partners in the supply chain. Anther point of view the is protection of the privacy of individuals.

Regarding the reliability and quality of service QoS for e-Business, the critical role of the IS security is one of the major business management responsibility. According to [4], the security encompasses the policies, the organizational procedures and technical measures used to guarantee a proper functioning of IS and protecting the enterprise against the consequences of malfunctioning. A guaranteed level of service performance should be delivered in accordance with Service Level Agreement SLA addressing the QoS of the source [4].

Regarding the trust in e-Business, where the contacts related to transactions occur by means of databases and computer networks, there are additional trade risks like: man-in-the-middle attack, spoofing, hacking, denial of service attacks, etc. The extent of this kind of attacks covers the manipulation of data, intentional use of a false identity or attacking the enterprise's portal. Therefore the security requirements imply the infrastructure availability, the network level protection and the message security.

Moreover, the transparency and audit-ability of the transactions, their non-repudiation and certification are the further needs. The message (information) security requirements demand a safeguarding of a user authentication. In addition, information integrity and confidentiality are also crucial. In this paper we concentrate on one chosen aspect of the message security – the user authentication which is a combination of claiming an identity and its verification proving that the identity is as claimed [4].

For user authentication as a one of the message security requirements, a broad spectrum of the guidelines, and approaches, are known and available [12]. For instance, the rules for a user authentication are defined in the Digital Authentication Guideline NIST SP [27]. In this publication the authentication of the user is defined as the process of assurance (assertion) of the identity of the users introduced to the system. Further, in Protecting Controlled Unclassified Information in NIST [26] there are lists with security requirements for identification and authorization services classified as two basic requirements, and eleven secondary, derived requirements. A common digital model for digital authentication as defined in [27] includes few key roles entities and some functions needed in the authentication procedure.

In the above model, if the requester addresses the registration authority RA to become a subscriber of the confidential service provider CSP, the registration authority RA is the trusted party, that ensures (states and credits) the identity of the user (requester). The credential is the data structure connecting the identity with additional verifiable attributes needed in the process of authentication of the claimant to the verifier. In the process of verification of user authentication there are four basic common way like: some information known to the person, some kind of things possessed by the person (referred to as a token), the aspects to the physical person (the static or/and dynamic biometrics). Generally the enumerated factors can be used in separation, or can be combined together. Nevertheless, there could be some problems with using of each method. Therefore the multifactor authentication is considered to be a proper solution. In the next Section we present our approach to the authentication problem.

V. EXAMPLES FOR USER AUTHENTICATION - PROPOSED SOLUTIONS

Regarding the GDPR Regulation and PSD2 directives, from which the requirements considering privacy and information security should be fulfilled by the information systems, in this Section we will give some subsequent examples of a possible user authentication processes by using the HTTP protocol [29] for authentication aims for Web-based applications. The HTTP protocol is commonly used by the implementation of the Web-applications; at present the recommendation for business is the usage the HTTP/2.0+ push protocol.

In Fig. 1 are depicted the three stages of the gradual development of this protocol - beginning with HTTP/1.1, then the following HTTP/2.0, to the HTTP/2.0+ push development stage. The development process of the subsequent stages has taken into account the aim of the minimization of the needed connections between the client and the server of a software application.

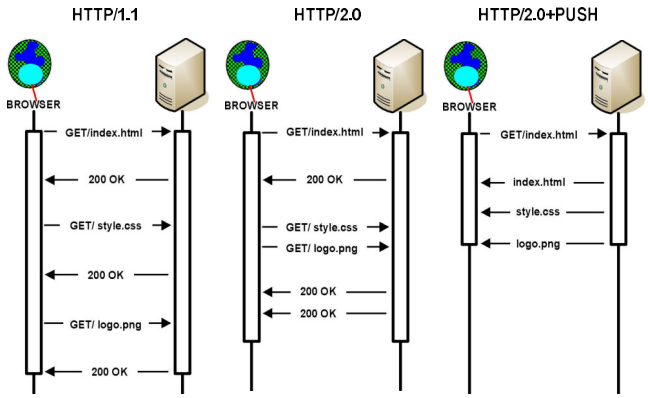

Fig. 1 Evaluation stages of HTTP protocol development

Using HTTP/1.1 protocol for opening of a Web page requires even three full transactions with the transmission of the elements containing the website descriptions. However, in the currently recommended version by W3C of the HTTP/2.0+ push protocol, the opening or refreshing of a website requires only one connection. The eliminating of unnecessary connections also significantly positive affects the security concerns, because it eliminates at the same time the possibility of seizing sessions and man-in-the-middle attacks to the necessary minimum, and this way reduces the risk of impersonating another users. It seems right, that good practices used in the development of HTTP, should also be utilized in systems applied for user authentication.

The second example is a simple authentication mechanism shown in Fig. 2, which uses only one single connection. This authentication method uses the asymmetric cryptography, also known as public key cryptography, which means, it uses public and private keys to encrypt and decrypt data. But in the process of the authentication the *Client* is using a secure private key denoted as ***prK*** and a secret password ***P*** to compute a cryptogram:

Cryptogram $\boldsymbol{S} = \boldsymbol{Crypt}(\boldsymbol{P}, \boldsymbol{prK})$.

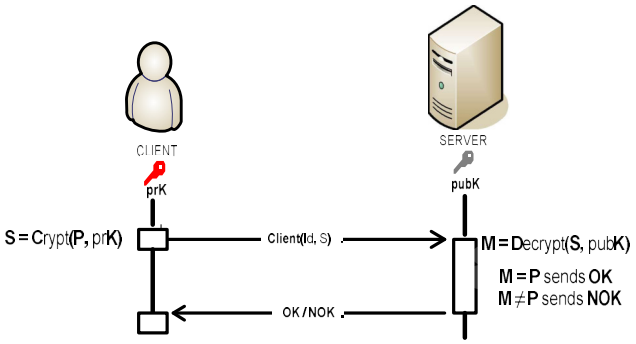

Fig. 2 Example of a simple authentication using asymmetric cryptosystems

The server, which knows the shared secret password ***P***, performs the decryption by using the public key ***pubK*** in the method ***Decrypt***(***S***, ***pubK***) and verifies if the shared secret is known by the client; the cryptographic function ***Crypt()*** is a known cryptographic algorithm with a public key. As a cryptographic algorithm proposed for the analysis aims we recommend the usage of the RSA schema described in [30]. In this method, as shown in Fig. 2, the authentication mechanism uses only a single connection.

However, this simple authentication method can not be regarded as secure, and is vulnerable to the various attacks by unauthorized users. A simple attack is presented in Fig. 3, where the hacker has an option of intercepting the cipher text ***S*** and so impersonating another user by using the captured cipher text. This method is referred to as sniffing accomplished by the Web communications and spoofing by another user.

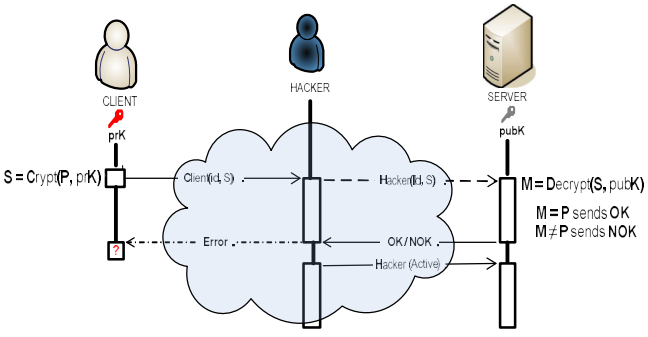

Fig. 3 The simple attack at authentication

The most secure authentication method is based on asymmetric cryptography and a cryptographic hash function named Hash [31]. This is a mathematical algorithm that maps data of an arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function, which is infeasible to be inverted [31]. The

proposed method uses the asymmetric cryptography and the cryptographic hash function - SHA2, in the authentication case shown in Fig. 4.

One must realize that removing parts of data will lead to results with lesser granularity, but this is a price, which must be paid to stay on the safe side and to stay compliant with the privacy rights.

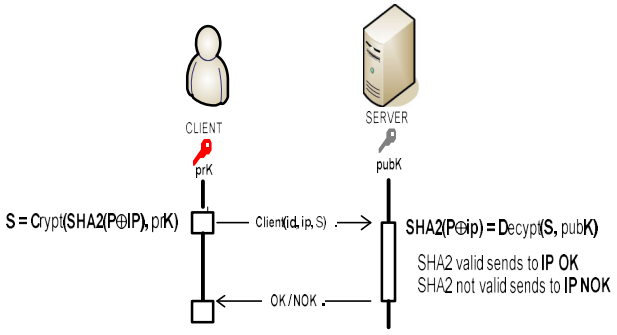

Fig. 4 Example authentication using asymmetric cryptosystems

In contrast to the known methods, which are using the hash function, in this solution the ***IP*** – the Internet protocol number was proposed as one of the input parameters for the hash function ***SHA2(P⊕IP)***. In this case the secret password *P* is aggregated with known ***IP*** and from this value a Client generates a cryptogram ***Crypt***(***SHA2***(), ***prK***). The proposed method is eliminating the possibility of simple spoofing, because this way we authenticate only the user, which has the valid ***IP*** number. However, acting according to this scheme does not protect against cryptanalytic attacks known to asymmetric cryptographic systems such as RSA.

In the scheme depicted in Fig. 4 we use a fixed cryptographic key, and this way we allow the off-line analysis of the private cryptographic keys.

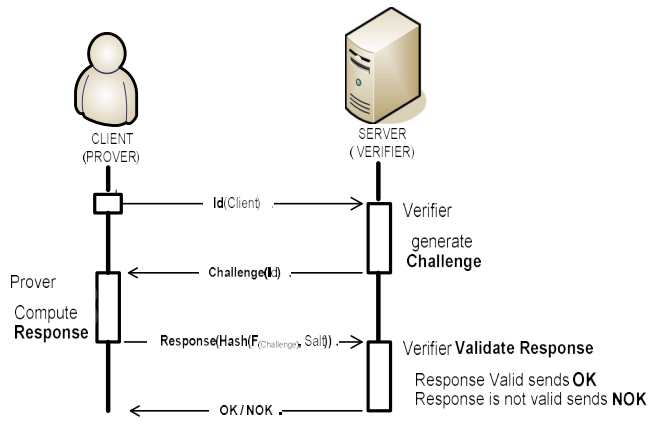

Fig. 5 Challenge-Response method in Client authentication method

In Fig. 5 there is a new situation depicted, where a Client uses an another authentication method named the Challenge-Response protocol. In this method only the hash functions are used; the method is used in OCRA. This method uses a constant function for a validation of the Response, and the Challenge can be regarded as variable value changing with each authentication.

In the last example (see Fig. 6) we give a proposal of Challenge-Response method based on the solution described in [20].

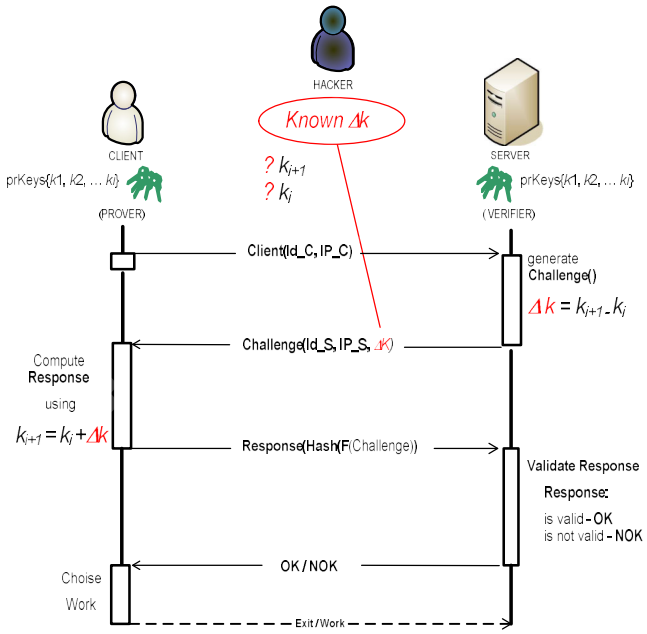

Fig. 6 Proposed Challenge-Response with OTP method in Client authentication

In Fig 6. a Challenge-Response authentication method is depicted, which is offering the perfect security of an authentication. In this solution, a high level of security is achieved through the authentication, which is using the advantages of OTP in asymmetric cryptography encryption and the hashing SHA2 method in the Challenge-Response mechanism. Additionally this proposal uses RSA, where the changeable shared value *prKeys* is a set of $\{k_1, k_2, \ldots, k_i\}$ and as a Challenge we are using the differential value $\Delta k = k_{i+1} - k_i$. In this case, even if someone is knowing the value Δk, it will be not possible to determine either the k_i or k_{i+1}.

The last shown method guarantees the semantic security, i.e. an adversary hacker can not gain even a partial information about an encrypted message (password) [32]. Therefore we recommend to undertake the user authentication in information systems collaborating in supply chains with usage of this method, as being the most appropriate for satisfying the requirements of cyber security, due to the EU regulations.

The last solution presented in this Section (depicted in Fig. 6) also conforms to the requirements of OTP and should be also resistant to the attacks with quantum computing, because, as stated above, the equation system given in the Fig 6 has no solution.

In this Section we gave some concrete examples for the authentication of the user (or processes) and also a proposal for an authentication of an information source, meeting the requirements ISO/IEC 2911, and also the European Directive from the 8th of September 2015 No. 1502 regarding the dynamically authentication.

VI. Conclusion

Already Alvin Toffler, Future Shock and Third Wave author, has indicated that the next phase of the industrial development will be the information society, where the information will have a particular value [33].

In the context of a rapid development of modern information technologies and digitalization, there is a growing importance of new factors that could threaten the security of logistics processes. It may be due to the wrong decisions caused by false (unreliable, insufficient, or incorrect) information, or caused by non-compliance with the required procedures or wrong (false) documents.

A solution trying to tackle such vulnerability problems is for instance a proposal of the COBIT 5 Information Security Framework for reducing cyber attacks on SCM systems [34]. However the COBIT framework does not take into consideration the concerns associated with the security of the authentication, which are based on the norms ISO/IEC 29115, and the European directive 1502/2015, as nowadays required.

According to [35] there are seven security concerns, which are addressing the main problems in contemporary supply chains: the inventory theft, the mismanagement of cloud access, the smuggling, the increased piracy, the physical device tampering, trusting data to a third party vendor, and the IoT Sensor compromise.

The physical threats like the smuggling or the piracy are out of scope of the considerations of this paper. The inventory theft is in fact a physical threat, however the credibility of the stocks of the inventories still remains important. The physical device tampering can cause the corruption of the data or disruption of the devices (or chips). Furthermore, the IoT sensor data represents an another possible attack vector.

From the above concerns particularly the mismanagement of cloud access due to an improper authentication could lead to serious security risks for supply chains. Therefore credibility of data, and also of the data sources, and on the other hand the audit-ability of the vulnerabilities of enterprise system are becoming crucial to guarantee the security in SCM.

Another important aspect, due to the GDPR is the preventing of data privacy for enterprises offering their services in the EU. In [36] the authors propose an approach for deriving Workflow Privacy Patterns from legal texts; these patterns are meant to support the designing of privacy compliant workflows.

In our paper we have shown some solutions as a proposal for complementing the tools with the elements of a secure authentication, that are also applicable in the context of a usage of the blockchain technology.

The design of software applications with respect to the demanded security and privacy requirements remains one of the current challenge for development and usage of Information systems. The new EU Regulation GDPR and PSD2 concerning the technologies used to support the banking and financial services Fintech, draw attention to the enhancement of required assurance level in security for processing sensitive data. The increasing numbers of incidents with the data leaks and an unauthorized access to digital resources or the denial of service (DOS) and other attacks are the symptoms of the raising problems with proper dealing with cyber security of the systems.

As a one most weak constituent in the system security considerations is the human factor which can not be so easily eliminated. In this paper we suggest the usage of the proper mechanisms, methods, and technologies that could be involved into the life cycle of are the Information systems, (as the constituents of supply chains) with the aim to increase the security of data and the transactions. Accordingly we have highlighted the importance of the deliberate choice of a software architecture, following the security rules during data exchange via computer networks, and also recommend a usage of the technologies, which are viable for a secure user authentication i.e., those with one-time keys.

In the examples in the last Section we have shown some possibilities for reducing the number of the required connections during the user authorization process in order to reduce a possibility of the hacker attacks.

The improvement of information security for information systems, can be achieved especially by using carefully chosen user authentication methods with the aim of fulfillment of the requirements of the high assurance levels of EU regulations.

The aim of this paper was to present the authentication methods conforming to the all three assurance levels given in [16]. The proposed solution presented in Section 5, in the last sixth example is a unique new solution, which fulfills the substantial and high assurance level of this EU Directive. The proposed method guarantees the realization of a dynamic authentication needs, as defined in this regulation and required by GDPR and PSD2. Thus we suggest the usage of this method in association with the technologies like block chain and cloud computing.

In the future we will further investigate the security aspects of Information systems and especially consider the diverse methods for a secure user authentication.

Currently recommended is the usage of HTTPS and TLS protocols with ecliptic curve sieve [37] with a small size of the encryption key. In the future we will consider the enhancement of this solution where the usage of RSA in the cryptography could be substituted by the application of the

elliptic curves or a lattice-based cryptography. Such solutions will be needed with the emerging quantum computing (post-quantum cryptography).

REFERENCES

[1] General Data Protection Regulation, "Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" EU 2016/679, 2016.

[2] Payment Services Directive 2, "Directive on payment services in the internal market", EU 2015/2366 Official Journal of the European Union Payment Service Directives 2. EU 2015/2366, 2015.

[3] Fintech: www.investopedia.com/terms/f/fintech.asp

[4] M. P. Papazoglou, and P. M.A. Ribbes, *E-business: organizational and technical foundations, John Wiley and sons*. London, 2006.

[5] L. Gil, and A. Liska, "*Security with AI and machine learning. using advanced tools to improve security at the edge*", New York O'Reily, 2019.

[6] Global Economic Crime and Fraud Survey, Pulling fraud out of the shadows. The biggest competitor you didn't know you had. 2018. https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

[7] D. Bohn, "Android at 10: the world most dominant technology", 2018 https://www.theverge.com/2018/9/26/17903788/google-android-history-dominance-marketshare-apple

[8] Hybrid warfare. Wikipedia https://en.wikipedia.org/wiki/Hybrid_warfare

[9] T. Magee, "*The most notorious hacke groups"*, ComputerworldUK https://www.computerworlduk.com/security/most-notorious-hacker-groups-3679258/

[10] G. Perkovitz and A. E. Levite, Eds., "*Understanding Cyber Conflict"*, Georgetown University Press, 2017.

[11] D. Sorin, The cyber dimension of modern hybrid warfare and its relevance for NATO Europolitcs, vol. 10-1, 2016. http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf

[12] W. Stallings, and L. Brown, "*Computer Security: Principles and Practice"*, Pearson Education 2018.

[13] OWASP Foundation. The free and open software security community, https://www.owasp.org

[14] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing", IEEE Transactions on Services Computing, vol. 5-2, April-June 2012, pp. 220 – 232, DOI: 10.1109/TSC.2011.24

[15] D. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng, and M. Baird, "Distributed ledger technology in payments, clearing, and settlement", Finance and Economics Discussion Series 2016-095, 2016. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095.

[16] Official Journal of the European Union. Technical Specification for assurance levels for electronic identification. 1502/2015EN.

[17] C. E. Schannon, "*Communication theory of secrecy systems"*, The Bell System Technical Journal, vol. 28-4 , Oct. 1949.

[18] L. Chen, S. Jordan, Y-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NISTIR 8105 Report on Post-Quantum Cryptography", http://dx.doi.org/10.6028/NIST.IR.8105 https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105

[19] Adips, *RUBLON, "Trusted access multi-factor authentication*", Zielona Góra, 2016. https://rublon.com/

[20] J. Jabłoński, "*Encryption system with one-off key"*, no. 218339, submitted 20-04-2011, date of the patent 10-09-2014.

[21] Project POIR .01.01.01-00-0257/16 - CryptOne unconditional secure crypto-processor, DCD Digital Core Design Bytom, Poland 2016-2019.

[22] J. Jasperneite, "*What is Industrie 4.0*", Computer&Automation, 2012

[23] S. Robak, B. Franczyk, and M. Robak, "Business process optimization with big data analytics under consideration of privacy", Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 8, p 1199–1204, 2016, DOI: http://dx.doi.org/10.15439/2016F542

[24] B. Schwarzbach, M. Glöckner, A. Pirogov, M. M. Röhling, and B. Franczyk, "Secure service interaction for collaborative business processes in the inter-cloud," in 2015 Federated Conference on Computer Science and Information Systems, ser. Annals of Computer Science and Information Systems, IEEE, 2015, pp. 1377–1386. http://dx.doi.org/10.15439/2015F282

[25] D. Agrawal, S. Das and A. E. Abbadi, „*Big data and cloud computing: current state and future opportunities*". EDBT 2011, March 22-24, 2011, Uppsala, Sweden. ACM 978-1-4503-0528-0/11/0003.

[26] RFC 6287 "OCRA: OATH Challenge-response algorithm", Internet Engineering Task Force IETF 2011, https://tools.ietf.org/html/rfc6287

[27] P. Grassi, M. Garcia, and J. Fenton, "Digital authentication guideline", NIST SP 800-63-3, 2016.

[28] R. Ross, K. Dempsey, P. Viscuso, M. Riddle, and G. Guissanie, "Protecting controlled unclassified information in nonfederal information systems and organizations" NIST SP 800-171, 2016.

[29] HTTP - Hypertext Transfer Protocol, https://www.w3.org/Protocols/

[30] S. Rivest,. A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Comm. of the ACM, vol. 21-2, 1978, pp. 120–126.

[31] B. Schneier, "Cryptanalysis of MD5 and SHA: Time for a new standard", Computerworld, 2014.

[32] S. Goldwasser, and S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences, vol. 28-2, 1984, pp. 270-299. https://doi.org/10.1016/0022-0000(84)90070-9

[33] A. Toffler, *The third wave*. Bantam Books, 1980.

[34] M. Wolden, R. Valverde, and M. Talla, "The effectiveness of COBIT5 information security framework for reducing cyber attacks on supply chain management system", IFAC-PapersOnLine Vol. 48-3, 2015, pp. 1846-1852. https://doi.org/10.1016/j.ifacol.2015.06.355

[35] L. Wainstein, "7 supply chain security concerns to address in 2019". https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-in-2019/

[36] M. Robak, and E. Buchmann, "Deriving workflow privacy patterns from legal documents", Federated Conference on Computer Science and Information Systems, 2019 – accepted paper.

[37] V. Gupta, D. Stebila, S. Fung, S.C. Shanz, N. Gura, and H. Eberle, "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography", http://research.sun.com/projects/crypto