Vojnotehnicki glasnik/Military Technical Courier

ISSN: 0042-8469

vojnotehnicki.glasnik@mod.gov.rs

University of Defence

Serbia

Manev, Nikola S.; Achkoski, Jugoslav Z.; Petresk, Drage T.; Goci, Milan Lj.; Rani, Dejan D.

Smart field artillery information system: model development with an emphasis on collisions in single sign-on authentication

Vojnotehnicki glasnik/Military Technical Courier, vol. 65, núm. 2, 2017, pp. 442-463

University of Defence

SMART FIELD ARTILLERY INFORMATION SYSTEM: MODEL DEVELOPMENT WITH AN EMPHASIS ON COLLISIONS IN SINGLE SIGN-ON AUTHENTICATION

Nikola S. Manev[a], *Jugoslav* Z. Achkoski[b], *Drage* T. Petreski[c], *Milan* Lj. Gocić[d], *Dejan* D. Rančić[e]

[a] University „Goce Delchev“, Military Academy „General Mihailo Apostolski“, Defence Resources Management, Skopje, FYR Macedonia,
e-mail: manev.nikola@yahoo.com,
ORCID iD: http://orcid.org/ 0000-0002-5591-4593

[b] University „Goce Delchev“, Military Academy „General Mihailo Apostolski“, Department for Security, Crisis Management, Protection and Rescue, Skopje, FYR Macedonia,
e-mail: jugoslav.ackoski@ugd.edu.mk,
ORCID iD: http://orcid.org/0000-0003-2782-3739

[c] University „Goce Delchev“, Military Academy „General Mihailo Apostolski“, Department for Security, Crisis Management, Protection and Rescue, Skopje, FYR Macedonia,
e-mail: drage_petreski@yahoo.com,
ORCID iD: http://orcid.org/0000-0002-5830-1389

[d] University of Niš, Faculty of Civil Engineering and Architecture, Niš, Republic of Serbia,
e-mail: milan.gocic@gaf.ni.ac.rs,
ORCID iD: http://orcid.org/0000-0001-8398-6570

[e] University of Niš, Faculty of Electronic Engineering, Department of Computer Science, Niš, Republic of Serbia,
e-mail: dejan.rancic@elfak.ni.ac.rs,
ORCID iD: http://orcid.org/0000-0002-3579-5654

https://dx.doi.org/10.5937/vojtehg65-12703

FIELD: Computer Sciences, IT
ARTICLE TYPE: Original Scientific Paper
ARTICLE LANGUAGE: English

Abstract:

This paper proposes a model for a Smart Field Artillery Information System (SFAIS) that can be used in a military environment. It is based on Service Oriented Architecture (SOA) and Command, Control, Communications, Computers, and Intelligence Information Systems (C4I), as well

as Geographical Information System (GIS) technology. The system aims to contribute in increasing the level of the military's capacity in the execution of operations in a multinational or a regional environment. In this context, the SFAIS provides a well-designed platform for interoperability with other actors in the same theater of military missions and joint operations. Moreover, the system will be used for educational purposes by being implemented in simulation centers and computer laboratories. This system will provide artillery personnel with proper education which will rely on - and is going to be conducted in - a simulated operational environment which will include the whole operational range of the artillery systems used (field of fire) and the process of preparation of the elements as well as conducting the firing in a virtual environment. Additionally,and even more importantly, the probability of collisions in hash functions during Single Sign-on authentication is presented for proving existing security shortcomings in distributed computer systems. Also, studying specific security issues with the SOA based artillery information system emphasizes the significance of applying a military information system in a security environment.

Key words: authentication, single sign-on, GIS, hash function, artillery, service oriented architecture, security, military, information systems.

Introduction

Field operations require a good understanding of the characteristics of the operational environment. Prior to using modern Information Technology (IT) systems, field crews relied exclusively on the guidance from a person that is familiar with the operational surrounding. If the teams or individuals were dispatched in a zone where the field activities were to be conducted without proper guidance, complex calculations needed to be performed using paper maps, compass and other devices in order to navigate and to fulfill the mission objective. Nowadays, with the development of contemporary Command, Control, Communications, Computers, and Intelligence (C4I) and Geographical Information System (GIS) solutions, organizations, companies and institutions are able to provide better support for their field crews not only in terms of navigation but in providing different spatio-temporal data including qualitative and quantitative characteristics of objects and events obtained during data collection, surveillance and intelligence activities as well. These information systems are usually tightly coupled with the Geographic Information System (GIS) which is a special type of computer-based information system tailored to store, process, and manipulate geospatial data (Worboys & Duckham, 2004) and is used to support command and control of operations starting from the tactical level up to the strategic level of armed conflict management. However,

the ability of the GIS to handle and process both location and characteristic data distinguishes the GIS from other information systems. This establishes the GIS as technologically important for a wide variety of applications (Chang, 2005), especially in the military domain. The GIS solutions are not only digital substitutions for paper maps but are becoming crucial in the integration of different information sources in a spatial context. The unique ability of the GIS to present different geo-referenced data on a map enables users to simulate different events through modeling, adjustment of data and scenarios for prediction, planning and estimation. In a spatial context, this level of information integration and presentation is difficult to achieve using any other information system. This is exactly why such systems can be and in recent times have a tendency to be used in a wide range of areas such as the security and intelligence domain, emergency management, and the military domain in particular. In a military environment, such systems are usually used for mission planning, target discovery and tracking, coordination between different military units and for weapon guidance and fire control.

In this paper, we propose a model for a specialized C4I system whose general purpose is artillery support. Considering the fact that similar systems require that geo-information as well as other types of information is accessible to a wide range of users with different responsibilities, located in different geographic locations, in addition to providing access to geospatial data for users with different levels of privileges and different responsibilities, this leads us to use Service Oriented Architecture (SOA) for developing a model of this type of system. Related work in this area is presented in the section that follows. Furthermore, the paper will deal with the phases of system development and look at the regulated access to the data that the Information system holds, in particular, the inconsistencies of using SOA regarding the probability that collisions can happen in hash functions during Single Sign-On (SSO) authentication with the stress of the Password Authentication Protocol (PAP). The expected results and conclusions are given at the end of the paper.

Related work

There are a large number of referred research papers from this area. Analyzing the relevant literature, we have come to the conclusion that in many technologically developed countries the implementation of Service Oriented Architecture in the military domain and especially in the Field Artillery Information Systems is driven by a unique reason - to enhance the

cooperation between different military actors on the battlefield and enhance their success while conducting a specific mission.

We can say with certainty that the latest achievements in the defense technology are based upon C4I (Command, Control, Communications, Computers, and Intelligence) (Worth, 2008) systems with Artillery Information Systems being a special kind of Command Information Systems (C4I) widely used by defense forces all over the World. Frequently used information systems, which support intelligence activities, have high influence in the decision making process, and modern information technology considerably contributes to the processes' improvement by supporting the intelligence cycles planning, collecting data, analyzing data and dissemination (Achkoski, et al, 2011). According to Medlow (Medlow, 2009), the interest about SOA leads to extended implementation in the information and communication systems that are a part of both the military and civil domain. However, we cannot simply implement Service Oriented Architecture (SOA) into the unchangeable infrastructure of an existing organization because there are numerous factors that can potentially complicate the implementation of SOA in the design of some systems within the military domain in spite our primary purpose being to enhance these systems (Pulier & Taylor, 2006).This is exactly why the effective implementation of SOA in the information systems of land forces detachments deployed in military, peacekeeping, post-conflict society reconstruction or any other kind of non-military jointly led missions presents a big challenge.

Radcliffe, et al. (Radcliffe, et al, 2014) conclude that the information systems for command and control that are used in the operational headquarters use SOA in order to increase the multiple actors' ability to exchange information between them. SOA's approach allows flexibility, integration, systems interoperability and increases the potential of the military actors using Commercial-Off-The Shelf (COTS) technology and standards. Moreover, this paper covers architecture modeling, SOA Governance and gives a summary of a specific multinational demonstration activity where these types of prototype services were implemented. The authors conclude that SOA solutions can be used for increasing the capability of specific actors acting in a clearly defined military environment. Furthermore, they propose developing SOA solutions of C4I information systems in every single field of the military environment.

The advancements of SOA in the development of information systems and the extent to which it helps for the effective use of directed military force is fully entailed under a program devised by the British, named: Network Enabled Capability (NEC). This problem matter is presented more clearly in (Brehm, Gómez, 2005, pp. 29-48).There we find that the

advancements of SOA can be exploited in building and designing military information systems for supporting NEC. Service orientation offers unique possibilities that ultimately change the way of exploiting information systems and with them the Ministry of Defense (MOD) departments and their operational formations can increase their efficiency.

Furthermore, from a business perspective, it is important to understand that the opportunity for the development of services focused on delivering improvements in the working capability of military actors will most certainly appeal greatly to potential customers and users. This same offer implies a solution in the form of an integrated system derived from the use of SOA planned to be used in line with the other, older information systems that are already used in the military.

Finally, this paper entails some of the exploits for SOA with the intention that the MOD will turn to using it more extensively and exploit the benefits of NEC on a higher level.

SFAIS model development

SOA presents a "next step" technology, steadily becoming a standard that inspires the re-use of information systems and loosely coupled systems. The independency of the implementation platform implies that older hardware and newer software can be replaced and updated without negative implications toward other components of a system as long as the communication interface of the service stays the same. Following the latest Information and Communication Technology (ICT) advancements, the Smart Filed Artillery Information System (SFAIS) based on SOA should be designed as a hybrid system (store-and-forward mode and real-time mode). The most recent research works and studies that address the use of SOA show that agencies, departments, institutions and other stakeholders can push and pull data in a standardized and flexible manner through the use of communication interfaces using XML schemes and web services.

The development of the SFAIS model based on SOA takes us through a number of phases. At the start, research will be focused on the wider "Information Technology and Military" expert public that will be asked to describe multiple solutions for information systems which will serve best and are related to the functions of artillery units. Because of the model sensitivity, this research will be focused on academic and unclassified sources, as well. As soon as that is done, an analysis whose purpose will be to make a conclusion about the benefits of modeling SOA based systems will take place in order to further strengthen the statement that SOA is the technological choice that

surpasses all other technological solutions for designing information systems of the C4I sort.

The actual design of the prototype starts with the development being focused on creating the basic system modules:

1. GIS Module - necessary for unit deployment in the operation planning phase when a specific artillery unit is being assigned a mission. The module presents the user with multiple variants of choice for deploying field artillery units (the combat component of artillery units) based on predefined parameters such as: deployment of the artillery battery combat elements – depending on the type of artillery weapon and deployment of the artillery division combat elements – depending on the type of artillery battery.

2. GIS based Forward Observer module - necessary to provide input data to the system. This module will be later used for further system development and testing. The Forward Observer (FO) module provides the user with basic functions for: marking positions of friendly and enemy units on a digital map, marking targets, targeting data, and transfer of target and fire mission data over the military network.

Figure 1 – Example from the mobile GIS Forward Observer module (the crossed, red, diamond shaped signs describe an enemy infantry unit)
Рис. 1 – Пример с модуля мобильной географической системы для поддержки артиллерии (маркировка в виде крестика, красного цвета и красного ромба обозначает пехотное подразделение противника)
Слика 1 – Пример из модула мобилног географског информационог система за артиљеријску подршку (ознаке у облику крста, црвене боје и дијаманта описују непријатељску пешадијску јединицу)

As a result of using the system modules, the possibilities of providing accurate information for deploying artillery weapons on the ground, especially in the region where artillery combat elements are scheduled for deploying, increase significantly (Figure 1). However, to calculate variables in the system module, the user will need to enter the following parameters: artillery weapon type, weapon caliber, ammunition type, region of targets, meteorological data, and other parameters. These parameters are a part of a different, Ballistic Module integrated within the Smart Field Artillery Information System, as shown in Figure 2.

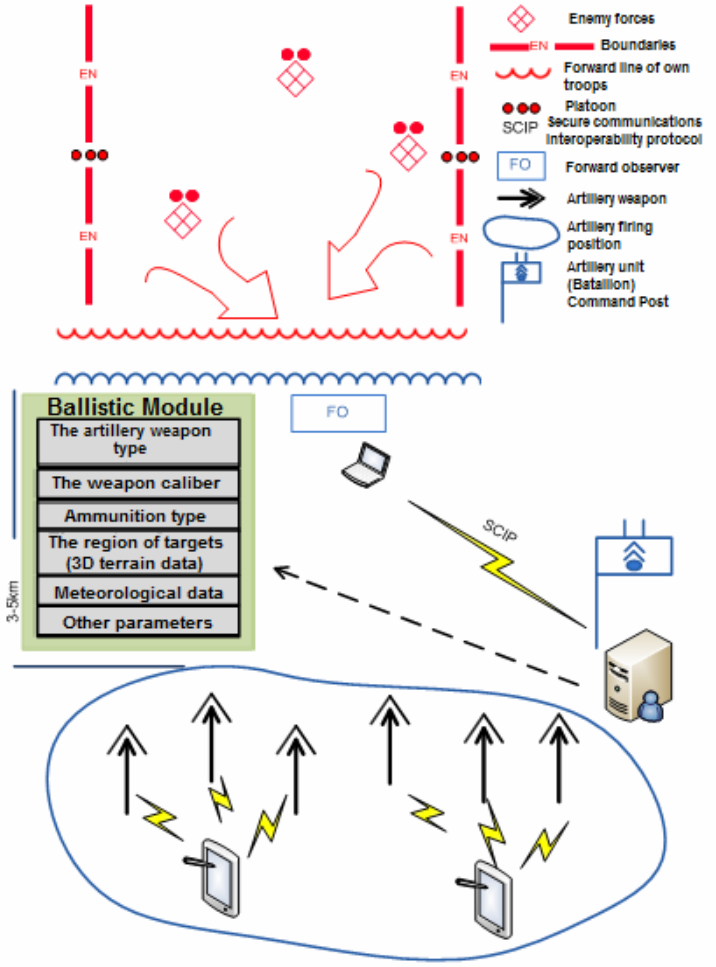

Figure 2 – Concept of the Smart Field Artillery Information System
Рис. 2 – Концепт интеллектуальной информационной системы полевой артиллерии
Слика 2 – Концепт паметног информационог система пољске артиљерије

Additionally, as the system development progresses on, a mathematical model will be defined and a Software Module will be designed to compute the initial or preparatory elements needed to direct the artillery fire. This module has different options (arranged in multiple optional categories) to choose from in order for the user to direct artillery fire while having the opportunity to select the type of weapon, the type of unit, and other options, which are important and must be taken in consideration to conduct a successful artillery firing.

The first category includes the subsystem for computing the preparatory or initial firing parameters for the artillery battery equipped with a certain type of weapon. The second category includes the subsystem for computing the initial firing parameters for an artillery division, which depends on the types of weapon within the different artillery batteries. The third category includes the sub-system for computing the parameters for subsequent corrections or the so-called adjusting of the artillery fire.

Moreover, a software module for the calculation of used ammunition per one artillery fire shooting will also be a part of the SFAIS. The module development automates the process for calculating used up ammunition. Furthermore, the module is connected to a military logistic information system that will provide timely reporting for used ammunition per firing and plan for timely supplying the artillery unit with the type of ammunition needed.

Finally, a protocol for exchanging information between the Forward Observer, the Fire Direction Center (FDC) and the Tactical Operational Center (TOC) will be used to channel information for exchange between these three pivotal actors on the battlefield. This information will provide a better visualization of the targets; it will fulfill the logistic requirements on time; it will help manage the human resources better, as well as significantly help the successful execution of the mission and operations.

In summary, developing the SFAIS would mean achieving the following goals in the field of directing artillery fire:

• Standardized protocol for exchanging information needed for achieving successful fire support;

• A defined application model that is easily integrated with other information systems that are not based on the service-oriented paradigm. Here we are avoiding the technical dependence for developing a field artillery information system relying only on one technology and, on the contrary, we are bringing in the possibility of integrating different information systems that are based on different platforms (Distributed Component Object Model – DCOM; Common Object Request Broker Architecture – CORBA; Remote Procedure Call – RPC; Remote Method Invocation - RMI);

Manev, N., et al, Smart field artillery information system: model development with an emphasis on collisions in Single Sign-On authentication, pp. 442-463

• A defined Integral Ballistic mathematical model for directed artillery fire which includes a weapon model, an ammunition type and ballistic parameters, meteorological data and a 3D terrain model;

• Integration of security mechanisms and a selection and description of security standards that should be used in the SFAIS in order to achieve an appropriate level of the access control;

• Defined metrics for the evaluation of the services related to the Field Artillery Unit implemented over service oriented architecture;

• Defined specific methodology for meteorological parameters determination based on the attenuation of electromagnetic waves in the atmosphere;

• Implemented desktop and mobile GIS front-end application for the visualization of SFAIS data.

Probability of collisions in hash functions during Single Sign-On authentication

Taking in consideration that the basis for the SFAIS prototype is Service-oriented architecture, we cannot stress enough the importance of looking at the pros and cons of using SOA as a platform for this system. Although SOA gives an unobstructed access to all actors with a specific clearance on using data, at the same time, as a platform, it faces a certain probability that collisions can happen in hash functions during Single Sign-On (SSO) authentication with stress on the Password Authentication Protocol (PAP). It means that clients (in a distributed computer system) or, in our case, actors on the battlefield with different privileges, can have access to services and resources that they are not authorized to use. To be more precise, what this means is that the distributed information system follows the well known matrix (*Table 1*) about the Discrete Authorization Control (DAC) system, a case where collisions that can happen in the system will cause the problem with the authentication and authorization in terms of system privileges that user have or do not have. Having stated that, here we are going to find the value of probability that depends on the length of the key (password) and the number of users in the system, where the results will be implemented in the PAP.

The Access Control Matrix (ACL) has subjects and objects. The subjects in the ACL are the users of the distributed system, in our case the users of services, where *S* is a row for every subject in the matrix. The objects in the ACL present system resources, where *O* is a column for every object in the matrix. The access allowed by the subject *S* to the object *O*

is stored in the intersection of the row indexed by *S* and the column indexed by *O*.The privileges in the system are shown in Table 1.

Table 1 – Access Control Matrix about Discrete Authorization Control (DAC);
x - execute; w - write; r - read; a - append
Таблица 1 – Матрица контроля доступа к дискретной авторизации (DAC);
x - исполнить; w - записать; r - прочитать; a - дополнить
Табела 1 – Матрица контроле приступа о контроли дискретне ауторизације (DAC);
x – извршити; w – написати; r – прочитати; a – додати

	/mail/Person X	edit.exe	db.exe
WS -1	{r, w}	{r, x}	{r, w, x}
Person X	{}	{r, w, x}	{w, x}
WS - 2	{a, r}	{}	{r, x}
. . .			
WS -N	{r, w}	{r, x}	{r, w}

The previously mentioned problem about collisions in the hash functions can be proven with the cryptography problem called *"birthday paradox"* as presented by (Batista, et al, 2012).The simplest way of presenting the security implications of hashing is with the question: How many people *K* out of *N* in one room have the same birthday as you if the probability is greater than 1/2? In order to find the probability *P(K)*, it is easier to compute the probability $\overline{P}$ of the number of people *N* that do not have the same birthday as you. The aforementioned authors come up with the following equations:

$$P(K) = 1 - e^{-\frac{N^2}{2*365}}$$

$$\ln 1 - \ln 2 = -\frac{N^2}{2*365} \Rightarrow N^2 = 2\ln 2 * 365$$

$$N = \sqrt{2\ln 2} * \sqrt{365} = 1.774 * 19.1045 = 23 \quad (1)$$

As far as the *"birthday paradox"* goes, we can conclude that 23 people in the room are enough to expect finding at least two or more people out of N to have the same birthday.

But, in addition to this, the *"birthday paradox"* can be exploited in computing the probability *P* of attacking the hash function, where the hash function *h(x)* generates an output of *N* bits long. In this case, the possible values of *N*, when *N* is used in the hash function *h(n)* , is 2^N, because *N*

could be either 0 or 1. Since $\sqrt{h} = \sqrt{2^N} = 2^{N/2}$ and if we hash about $2^{N/2}$ different inputs, we can expect to find a collision, that is, have two inputs that hash to the same value.

For example, if we want to find the work that needs to be done in order to break the hash function with a probability of 0.5 for generating a collision with brute force, where the input is the hash function with 32 *bits*, then we need to compute:

$$N(0.5,h) \approx 1.1774 * \sqrt{h} \Rightarrow$$

$$\Rightarrow 0.5 - \text{Probability to break hash function}, \sqrt{h} = 2^{N/2}$$

$$N\left(\frac{1}{2},32\right) \approx 1.1774 * 2^{\frac{32}{2}} = 1.1774 * 2^{16} = 1.1774 * 65536 = 7.7 * 10^4 \qquad (2)$$

Finally, we need to discuss the collisions that can happen with brute force with different values of probability that depend on the number of *n* bits in the hash function *h(n)*. In this case, we are looking at two cases (Case A and Case B). The numbers of bits that are used in these cases are 64, 80, 128 and 160 *bits*. The particularity in the selection of using these numbers of bits refers to the standard length of a password, which means that 8 characters is the standard length of a password. However, the user can choose from 256 possible characters from the keyboard. The choices that the user has can be presented as 256^8. This number is equal to 2^{64} hash function *h(n)* or it is a 64-bit cryptographic key, hence the reason for choosing $n = (64,80,128,160)$ as a length for the hash function *h(n)*.

To illustrate the real time working capability of a SOA platform as well as the hash function application, it is best to provide a real-life example of an Information system whose access is open only to users with a specific clearance, authorized by an account and a password.

Example: Let us suppose that we designed a multi user information system based on service-oriented architecture. The information system is accessed by multiple users based on their account and their password. If the system administrator records the accounts and passwords in a separate file in the information system, then the level of threat is too high. One of the solutions to this problem is saving user names and passwords that are hashed with a certain hash function *h(n)* in a separate file. Let us assume that the hash function *h(n)* is an ideally and perfectly chosen function, where *h* maps each valid input into a different hash value $\{0.,1\}^* = \{0.,1\}^k$. This means that users access the system with *n* passwords and the Information system allows access to the user in the system only if the hash va-

lue *h(n)* can directly locate the record in the file where the hash values are stored.

Case A: If we have an attacker (a regular user) that has the intention of accessing the computer system as a system administrator (super user) generating random passwords (avoiding duplication of passwords that are used once), what are the minimum numbers of passwords *(N)* that the attacker can try to guess correctly?

To explain Case A in an appropriate manner, the following assumptions are introduced:

$$n = 64 bits \ ; \ P = 25\% \ ; \ P = 50\% \ ; \ P = 75\% ; \ P = 99\%$$

To determine the probability of collisions, when the password is 64 bits long, we have to compute the following expression:

$$P = 99,9\%; \ n = 64 bits \Rightarrow h = 2^{64}$$

$$\Rightarrow 0.99 = 1 - e^{-\frac{N^2}{2h}} \Rightarrow 0.01 = 1 - e^{-\frac{N^2}{2h}} \ / ln$$

$$\ln 0.01 = -\frac{N^2}{2h} \Rightarrow N^2 = -2 * \ln 0.01 * h$$

$$\ln 0.01 = -4.605170185988091 \approx -0.4606$$

$$-2 * \ln 0.01 = -2 * (-4.606) \approx 9.212$$

$$N = \sqrt{9.212} * \sqrt{h} = 3.035 * \sqrt{2^{64}} = 3.035 * 2^{32} = 3.035 * 4.3 * 10^9 = 13.05 * 10^9$$

Table 2 showcases the results for the desired probability when the passwords are 64 *bit* long. The intention is not to show how the process of computation is done and that is the reason that we show only how the probability is computed with 99%. Since the same equation can be used in order to calculate the desired probability when the passwords are 64, 80 and 128 *bits* long, the results in the remaining 3 cases are respectively presented within Table 2, as well.

Table 2 – The results of the desired probability when passwords are 64, 80, 128 and 160 bits long
Таблица 2 – Результаты предполагаемой вероятности, в случае длинных паролей 64, 80, 128 и 160 битов
Табела 2 – Резултати жељене вероватноће када су лозинке дугачке 64, 80, 128 и 160 бита

	Probability of collisions with the brute force attack			
Number of bits	$\left(\frac{1}{4}\right)25\%$	$\left(\frac{1}{2}\right)50\%$	$\left(\frac{3}{4}\right)75\%$	99%
64	$3.3*10^{9}$	$5,06*10^{9}$	$7.2*10^{9}$	$13.05*10^{9}$
80	$0.82*10^{12}$	$1.28*10^{12}$	$1.8*10^{12}$	$3.3*10^{12}$
128	$1.4*10^{19}$	$2.2*10^{19}$	$3.1*10^{19}$	$5.46*10^{19}$
160	$0.60*10^{24}$	$1.41*10^{24}$	$1.99*10^{24}$	$3.6*10^{24}$

In response to the conclusion we have made earlier, let us repeat that the number of bits used in these cases are 64, 80, 128 and 160 bits. The particularity in the selection of using these numbers of bits refers to the standard length of a password, which means that 8 characters is the standard length of a password. However, the user can choose from 256 possible characters from the keyboard. The choices that the user has can be presented as 256^8. This number is equal to 2^{64} hash function *h(n)* or it is a 64-bit cryptographic key; hence the reason for choosing $n=(64,80,128,160)$ as a length for the hash function *h(n)*. Accordingly, a graphic presentation is given for each and every possibility of a 64, 80, 128 or 160 bit password length in Figures 3, 4, 5, and 6, respectively. Figure 7 gives a cumulative graphic presentation of the password length of *n* = (64,80,128,160) *bits*.

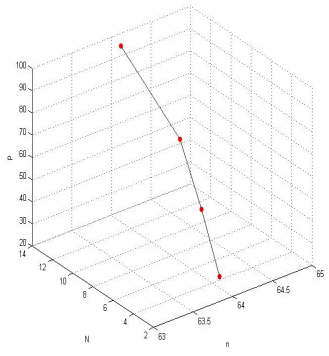

Figure 3 – A 3D graphic presentation for the password length of *n = 64 bits*
Рис. 3 – 3Д графическое изображение пароля размером *n = 64 битов*
Слика 3 – 3Д графичка презентација за лозинку дужине *n = 64 bits*

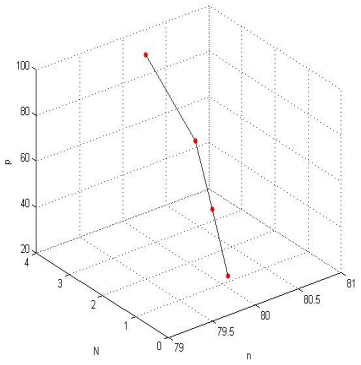

Figure 4 – A 3D graphic presentation for the password length of *n = 80 bits*
Рис. 4 – 3Д графическое изображение пароля размером *n = 80 битов*
Слика 4 – 3Д графичка презентација за лозинку дужине *n = 80 bits*

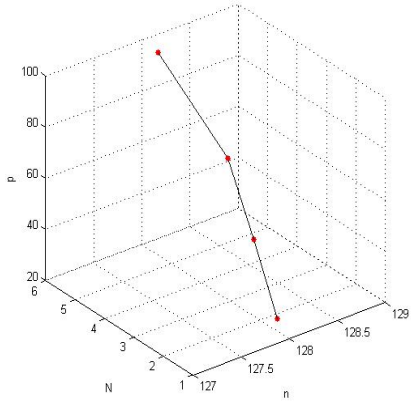

Figure 5 – A 3D graphic presentation for the password length of *n = 128 bits*
Рис. 5 – 3Д графическое изображение пароля размером *n = 128 битов*
Слика 5 – 3Д графичка презентација за лозинку дужине *n = 128 bits*

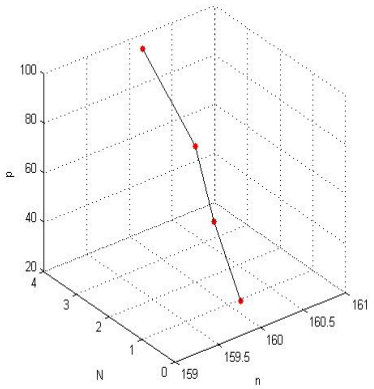

Figure 6 – A 3D graphic presentation for the password length of *n = 160 bits*
Рис. 6 – 3Д графическое изображение пароля размером *n = 160 битов*
Слика 6 – 3Д графичка презентација за лозинку дужине *n = 160 bits*

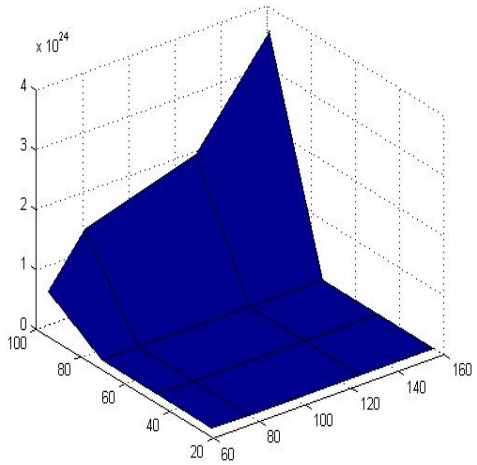

Figure 7 – A 3D graphic presentation for the password length of *n = (64, 80, 128, 160) bits*
Рис. 7 – 3Д графическое изображение пароля размером *n = (64, 80, 128, 160) битов*
Слика 7 – 3Д графичка презентација за лозинку дужине *n = (64, 80, 128, 160) bits*

Additionally, we created a pseudo code for computing collisions in the hash function that can help optimize the process for gathering value of trays that depend on the probability and bits in the hash function.

Computing collisions(){

declare variables (){

variable P;

input $\mathrm{P} = (0,\ldots,1)$;

variable n;

input $\mathrm{n} = (0,\ldots,n-1,n)$;

}

compute $h(n)$ (){

$\mathrm{h}(\mathrm{n}) = 2^{\mathrm{n}}$

return $\mathrm{h}(\mathrm{n})$;

}

initialize computation(){

$$P = 1 - e^{-\frac{N^2}{2*h}}$$

do substraction () {

$$e^{-\frac{N^2}{2*h}} = 1 - P$$

$$e^{-\frac{N^2}{2*h}} = P'$$

if (P' *is greater than* 1){

Print " *Algorithm failed* "

else{

if (P' *is less or equal to* 1){

Print " *Continue with computation* "

}

}

return P'

}

start natural logarithm function (){

$\log_e x = \ln x$;

$$e = 2.718;$$

divide expression with natural logarithm ln (){

$$e^{-\frac{N^2}{2*h}} = P' \ / \ln$$

$$\ln P' = -\frac{N^2}{2*h}$$

return P'

}

compute expression(){

$$2 * \ln P' * h = -N^2$$

$$N^2 = -2 * \ln P' * h$$

$$N = -\sqrt{2 * \ln P'} * \sqrt{h}$$

compute : $-\sqrt{2 * \ln P'} = a;$

compute : $\sqrt{h} = 2^{\frac{n}{2}} b;$

return a, b ;

replace a *and* b ;

$N = a * b;$

return N;

}

END

Case B: What is the maximum number of users *(N)*, when the probability of a collision with brute force happening in the system is under 0.05%? It means that the probability of a hash function, where every pair of users has the probability of matching passwords, is equal to 0.05% .

To compute the number of users in the system with certain probability of collisions with brute force in Case B, we have introduced the following assumptions:

1) $n = 64 bits \ ; h = 2^{64} \ ; P = 0.05\% \ ; N(0.05\%) = ?$
2) $n = 80 bits \ ; h = 2^{80} \ ; P = 0.05\% \ ; N(0.05\%) = ?$
3) $n = 128 bits \ ; h = 2^{128} \ ; P = 0.05\% \ ; N(0.05\%) = ?$
4) $n = 160 bits \ ; h = 2^{160} \ ; P = 0.05\% \ ; N(0.05\%) = ?$

Manev, N., et al, Smart field artillery information system: model development with an emphasis on collisions in Single Sign-On authentication, pp. 442-463

Consequently, Table 3 portrays the maximum number of users in the system to avoid collisions while *P = 0.05%* and Figure 8 relates to these results.

Table 3 – The maximum number of users in the system to avoid collisions, while *P = 0.05%*
Таблица 3 – Максимальное количество пользователей в системе, установленное с целью предотвращения коллизий, при *P = 0.05%*
Табела 3 – Максимални број корисника у систему да би се избегле колизије када је *P = 0.05%*

	Association of the number of bits in passwords and number of users in correlation with limited probability of collisions			
Limited Probability of collisions with the brute force attack	64	80	128	160
0.05%	$1.3*10^{9}$	$0.34*10^{12}$	$0.59*10^{19}$	$0.39*10^{24}$

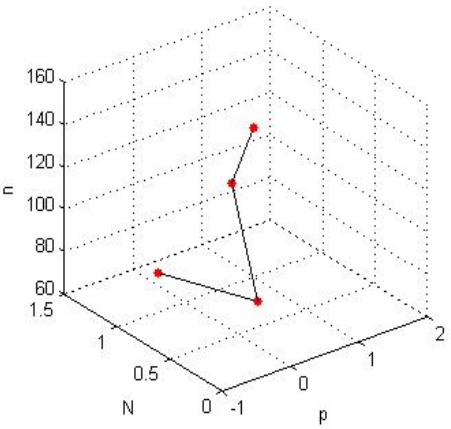

Figure 8 – A 3D graphic presentation for maximum number of users with *P = 0.05% and n = (64, 80, 128, 160)*
Рис. 8 – 3Д графическое изображение количества пользователей при *P = 0.05%* и *n = (64, 80, 128, 160)*
Слика 8 – 3Д графички приказ за максимални број корисника када је *P = 0.05%* и *n = (64, 80, 128, 160)*

Conclusion

On the positive side, innovations are tightly related to this system's creation because they refer to the shift from a traditional way of directing artillery fire into a contemporary and technologically sophisticated way of directing artillery fire. The system makes most of the processes automatic in the moment of firing from a field artillery unit deployed in the battlefield. In that manner, the field artillery units which will be equipped with SFAIS will be capable of opening artillery fire on predefined and planed enemy targets far more effectively, increasing the probability of getting an accurate artillery shot on target, excluding errors caused by the human factor during the process of preparing and entering the parameters for directed fire.

Moreover, implementing the SFAIS prototype in field artillery units is going to contribute to increasing the level of military capability while executing operations in a multinational or regional environment. In the same context, SFAIS is providing a well-designed platform for interoperability with other actors in the same theater of military missions and joint operations. The system will also make a new and significant contribution in joint operations and homeland security through the possibility of exchanging information in an appropriate way, decreasing the time for fire support in military operations and missions, disseminating information to authorities enhancing the decision-making process and taking appropriate actions, all in a faster and more reliable manner.

In addition, the system will be exploited for educational purposes. Implementing it in simulation centers, computer laboratories and other facilities will provide affordable education for artillery personnel by simulating field artillery firing and executing the process of firing in a virtual environment. Artillery officers, cadets and other personnel from the artillery branch will not need to use real time artillery weapons, military training fields and other equipment, because the system will allow the training for directing artillery fire to be executed in a lab or in a simulation center. As a result, this will allow for the justified promotion of field artillery experts capable of bringing timely and accurate decisions for resolving situations

On the "not entirely" negative side, the computation of probability of collisions in hash functions demonstrates the weaknesses in the system security, where user who do not have privilege can access system resources. We can firmly conclude that the collisions in hash functions during an SSO authentication are possible and likely to happen, but the results for finding a collision and breaking the hash function *h(n)* show that a lot of work has to be done. The work of finding collisions in hash functions is

Manev, N., et al, Smart field artillery information system: model development with an emphasis on collisions in Single Sign-On authentication, pp. 442-463

equivalent to the work of a brute force exhaustive key search. However, the results of our theoretical research prove that the probability of collisions in the system can decrease the level of security in the system, but this is easily overcome by the users who do not select random passwords and follow the guidelines for PAP.

References

Achkoski, J., Trajkovik, V., & Davcev, D., 2011. Service-Oriented Architecture Concept for Intelligence Information System Development. In: Proceedings of the Third International Conferences on Advanced Service Computing SERVICE COMPUTATION 2011 (IARIA), Rome.

Batista, E., Canal, G., & Ziadeh, K., 2012. The birthday paradox: Operational research and optimization.

Brehm, N., & Gómez, J.M., 2005. Secure web service-based resource sharing in ERP networks. *International Journal on Information Privacy and Security (JIPS),* 1.

Chang, K., 2005. Introduction to Geographic Information Systems, 3rd ed.New York, NY: McGraw-Hill.

Medlow, D., 2009. Saab Systems: Extending service orientated architectures to the deployed land environment. In: Proceedings of the Military Communications and Information Systems Conference (MilCis), Australia.

Pulier, E., & Taylor, H., 2006. *Understanding enterprise SOA*.MANNING.

Radcliffe, S., Trotman, L., & Duncan, H., 2014. Supporting capability evolution using a service oriented architecture approach in a military command and control Information system.

Worboys, M., & Duckham, M., 2004. *GIS: A Computing Perspective, 2nd ed*.Boca Raton, FL: CRC Press.

Worth, B.J., 2008. Command, Control, Communications, Computers, and Intelligence (C4I Interoperability: Are We There Yet? Faculty of the U.S. Army Command and General Staff College. MasterThesis.

ИНТЕЛЛЕКТУАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ПОЛЕВОЙ АРТИЛЛЕРИИ: РАЗРАБОТКА МОДЕЛИ С АКЦЕНТОМ НА КОЛЛИЗИИ В АУТЕНТИФИКАЦИИ SINGLE SIGN-ON

Никола С. Манев[а], *Югослав* З. Ацкоски[б], *Драге* Т. Петрески[в], *Милан* Л. Гоцич[г], *Деян* Д. Ранчич[д]

[а] Университет «Гоце Делчев», Военная академия «Генерала Михаило Апостолоски», Управление ресурсами обороны, Скопье, БЮР Македония
[б] Университет «Гоце Делчев», Военная академия «Генерала Михаило Апостолоски», Кафедра безопасности и защиты в кризисных и чрезвычайных ситуациях, Скопье, БЮР Македония
[в] Университет «Гоце Делчев», Военная академия «Генерала Михаило Апостолоски», Кафедра безопасности и защиты в кризисных и чрезвычайных ситуациях, Скопье, БЮР Македония
[г] Университет в г. Ниш, Архитектурно-строительный факультет, г. Ниш, Республика Сербия
[д] Университет в г. Ниш, Факультет электроники, Кафедра вычислительной техники, г. Ниш, Республика Сербия

ОБЛАСТЬ: КОМПЬЮТЕРНЫЕ НАУКИ, IT
ВИД СТАТЬИ: оригинальная научная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

В данной статье представлена модель интеллектуальной информационной системы полевой артиллерии (SFAIS), разработанная для военных целей и основанная на сервисно-ориентированной архитектуре (SOA), а также на C4I информационной системе и технологии географической информационной системы (GIS). Цель внедрения системы заключается в повышении уровня мощности вооруженных сил при выполнении операций в рамках многонациональных или региональных действий.В этомпланеSFAIS обеспечивает хорошо спроектированную платформу для взаимодействия с другими участниками совместных военных миссий вколлективных операциях.

Система разработана для применения в центрах моделирования и симуляции, а также в лабораториях. Данная система будет применяться в учениях артиллерийских подразделений, в смоделированных операционных условиях, которые включают целый спектр артиллерийской системы (артиллерийский огонь), а также наводку орудий и выполнение огневых задач в виртуальных условиях.

Наряду с вышеперечисленными задачами, будет представлена вероятность коллизий в хешировании приSingleSign-on аутентификации, с целью выявления недостатков в системе безопасности компьютерных сетей.

Исследования специальных параметров по безопасности артиллерийской информационной системы основаны на сервисно-ориентированной архитектуре, что в свою очередь подчеркивает значимость применения информационной системы военной безопасности.

Ключевые слова: аутентификация, single sign-on, GIS, хеширование, сервисно-ориентированная архитектуря, безопасность, вооруженные силы, информационные системы.

ПАМЕТНИ ИНФОРМАЦИОНИ СИСТЕМ ПОЉСКЕ АРТИЉЕРИЈЕ: РАЗВОЈ МОДЕЛА С ТЕЖИШТЕМ НА КОЛИЗИЈЕ У SINGLE SIGN-ON АУТЕНТИФИКАЦИЈИ

Никола С. Манев[а], *Југослав* З. Ацкоски[б], *Драге* Т. Петрески[в], *Милан* Љ. Гоцић[г], *Дејан* Д. Ранчић[д]

[а] Универзитет „Гоце Делчев", Војна академија „Генерал Михаило Апостолоски", Управљање ресурсима одбране, Скопље, БЈР Македонија

[б] Универзитет „Гоце Делчев", Војна академија „Генерал Михаило Апостолоски", Катедра за безбедност, кризни менаџмент, заштиту и спасавање, Скопље, БЈР Македонија

[в] Универзитет „Гоце Делчев", Војна академија „Генерал Михаило Апостолоски", Катедра за безбедност, кризни менаџмент, заштиту и спасавање, Скопље, БЈР Македонија

[г] Универзитет у Нишу, Грађевинско-архитектонски факултет, Ниш, Република Србија

[д] Универзитет у Нишу, Електронски факултет, Катедра за рачунарство, Ниш, Република Србија

ОБЛАСТ: рачунарске науке, IT
ВРСТА ЧЛАНКА: оригинални научни чланак
ЈЕЗИК ЧЛАНКА: енглески

Сажетак:

У раду се предлаже модел паметног информационог система пољске артиљерије (SFAIS) за примену у војне сврхе. Заснован је на сервисно оријентисаној архитектури (SOA), као и на C4I информационим системима и технологији географског информационог система (GIS). Циљ система јесте да допринесе повећању нивоа капацитета војске при извођењу операција у мултинационалном или регионалном окружењу. У том контексту SFAIS обезбеђује добро пројектовану платформу за интероперабилност с осталим учесницима заједничких војних мисија и здружених операција. Штавише, систем ће бити коришћен за едукацију у центрима за симулацију и компјутерским лабораторијама. Артиљерцима ће обезбедити едукацију засновану на симулираном оперативном окружењу, у којем ће се и изводити, а

које ће обухватати читав операциони спектар артиљеријских система (артиљеријске ватре), као и процес припреме елемената и извођење гађања у виртуелном окружењу. При томе ће, што је још важније, представити вероватноћу колизија у хеш функцијама током single sign-on аутентификације како би се показали постојећи сигурносни недостаци у дистрибуираним компјутерским системима. Проучавање специфичних сигурносних момената код артиљеријског информационог система, заснованог на сервисно оријентисаној архитектури, такође истиче значај примене војног информационог система у сигурносном окружењу.

Кључне речи: аутентификација, single sign-on, ГИС, хеш функција, артиљерија, сервисно оријентисана архитектура, сигурност, војска, информациони системи.

Paper received on / Дата получения работы / Датум пријема чланка: 28.12.2016.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 19.03.2017.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 20.03.2017.