The Security of the Mobile Citizen Oriented Applications

Ion IVAN, Adrian VISOIU, Silvia TRIF, Bogdan VINTILĂ, Dragos PALAGHITĂ
Academy of Economic Studies, Bucharest, Romania
ionivan@ase.ro, adrian.visoiu@csie.ase.ro, silvia.trif@stud.ase.ro, vb@vintilabogdan.ro, mail@dragospalaghita.ro

The concept of citizen oriented informatics application is defined. The differences between these and the traditional applications are described. Structures of citizen oriented applications are presented. The development cycle of the citizen oriented applications is followed and foe each step, differences from the traditional development cycle of the applications are underlined. The security requirements of the citizen oriented applications are discussed. Vulnerabilities of the applications are described. Ways of dealing with vulnerabilities are discussed. The limitations of the mobile devices are highlighted. The authentication process and the automation of it are taken into discussion. An authentication method based on gestures recorded from accelerometer sensor data is proposed as simple and effective way for accessing application resources.

Keywords*: citizen oriented applications, mobile applications, security, vulnerabilities, distributed applications, gesture based authentication, accelerometer data, neural networks*

1 Citizen oriented informatics applications

In the context of the knowledge based society and of higher citizen requirements the appearance of a new category of informatics applications is necessary. The citizen orientated applications bring a new orientation as the citizen is considered to be the central element. These differ from the classic applications through [1]:

- these are developed to solve the problems of the citizens, not the problems of the organization for which are developed;
- the target group is very large and very divers being formed by all the citizens;
- the applications are always available online;
- the citizen oriented applications aren't dependent on the hardware or software platform;
- the cost of use is very low or null;
- certain quality requirements are much more strict than for traditional applications; usability is a quality characteristic that, in time, determines the acceptance of the software product; the product must be designed such way that people of various ages, various education to be able to interact with the application and obtain desired results, otherwise it will lose its purpose of being used by all citizens; security is also an important quality characteristic that represents the ability of the application to protect sensitive personal information as users divulge such information when filling request forms or apply to services; complexity is quality characteristic that it is important to be as low as possible at interface level, and high at logic level as it is correlated to a high level of functionality obtained with minimum input interaction;
- localization assumes having the dialog with the user in his own language;
- the use of the applications doesn't assume previous training of the users [2];
- are very often updated to reflect the changes in the environment;
- adaptation to offer the citizens a greater degree of satisfaction.

The structure of the citizen oriented informatics applications differ on the offered functionality and the domain they are created for. The citizen oriented informatics applications are with:

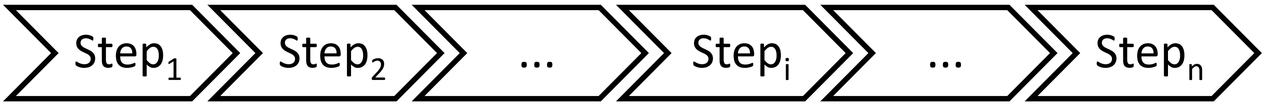


Fig. 1. Simple linear structure

- simple linear structure; these are applications that, for problem solving, assume the following of a number of steps, in a preset order, without the possibility to go back to a previous step; the structure is showed in Fig. 1;
- linear structure and simple links between components; these assume the possibility of going back to the previous steps;
- linear structure and multiple links; assumes the existence of links between components and the navigation is made between any of the connected components respecting limitations imposed for the correct functioning of the application; the navigation towards a step is not allowed without the fulfillment of the prerequisites;
- tree structure and simple links; these are applications for which from a step the user can move in many directions;
- tree structure and double links; these assume the existence of bidirectional links between the components to browse the tree structure both top-bottom and bottom-top;
- tree structure and multiple links; the pass from a component to another is made only in the limit of the good functioning given by the logic of the processing which the applications make.

The distributed informatics applications are the result of a complex process that includes steps characterized by [3]: specific objectives in each of them, input elements, activities, resources [4], techniques, methods, technologies, results.

The steps of the development cycle of the citizen oriented informatics applications differ when compared with the same steps of the classical applications because the focus is on the citizen orientation as the application must reflect the needs and preferences of the citizens.

Problem definition step assumes specialists with high experience in the knowledge of the theoretical aspects and also, very important, of the practical ones, from the domains with which the application interacts.

Establishing the target group is the step in which the categories of persons that interact with the application for problem solving is set and the number of individuals is estimated.

Specifications elaboration is the step that assumes the existence of specialists of high performance with rich experience because the specifications must be [5] exact, complete, correct, deterministic.

Project building is the step in which experienced specialists in results interpreting and code elaboration start identifying processing functions, setting modules and their links, defining data structures and storing format, building matrixes of initial data – modules and final results – modules, establishing software and hardware necessary resources, estimating the workforce, elaborating a calendar specific to the development of the application.

Code elaboration is an activity through which a project is materialized and competed by developers with great experience in the chosen technologies, which possess the capacity of taking information from specifications so that the written lines of code represent standalone products whose quality is measured exactly.

Server loading is preceded by an analysis made by a small group of specialists of the developing team.

Technical testing is preceded by autotesting. This means that the product already fulfills the requirements from the specifications [6].

Sample testing assumes the establishment of the persons that, with specialized assistance, solve real problems using the distributed application.

Documentation elaboration is an activity that is, erroneous, left for the end of the development cycle by the majority of the development team members. The documentation must be built simultaneously with the development process even if that is not the final form of it [7].

Implementation assumes the installation of the application on the client's server and the configuring for optimum functioning.

Maintenance is the process of updating the citizen oriented applications to reflect the changes from the economic, social and legislative environment and also fixing the defects that were discovered after the release.

Software reengineering assumes the redefining of the application's objective so that it leads to increases of quality and performance, but the new objective is not totally different from the original one.

Removal from use is a rare process as many applications don't pass the maintenance and reengineering processes.

2 Security requirements for the citizen oriented applications

Citizen oriented informatics applications differ from the other informatics applications, determining a series of particularities because [8]:

- the applications are freely accessed because there are no more geographical borders and the users must be able to access the applications anytime without additional costs [9];
- the complexity of the citizen oriented applications is very high as these are distributed applications and their development overwhelms the classic approach;
- the users are many and diverse because the citizen oriented informatics applications reach their aim only if they are used by many persons;
- the processing fluxes are saturated given the large number of users and the complexity of the applications;
- the security level is uniform for all the branches of the tree associated to the application usage and there are no known security breaches left after testing phase; in current use, security problems are recorded and solved with high priority;
- the management of the database and the files of the application is made through procedures that exclude processing incidents.

The citizen oriented informatics applications are affected by vulnerabilities:

- authentication of unauthorized persons;
- SQL injections are also a great vulnerability for the citizen oriented informatics applications;
- public access is also a vulnerability for the applications that are public as all persons are allowed to use it and they can discover bugs that passed the testing process;
- the exposure of many web services can create backdoors for malicious persons [10];
- the high complexity of the citizen oriented informatics applications leads to a big development team; each member of the development team has knowledge of the functioning of the application and if the right occasion or reason appears they can exploit it;
- hardware failure is one of the causes that leads to the total failure of the distributed applications.

The vulnerability list is not exhaustive and more vulnerabilities can be added. The important thing is that these are taken into account at the development of the citizen oriented informatics applications. The vulnerabilities are divers but all of them can be solved.

The increase in security is made through:

- insertion of components that eliminate vulnerabilities; patches to the application add protection from discovered vulnerabilities such as buffer overflow attacks that may occur at a single function level from a module; installation of patches is done under maintenance by replacing the affected modules in a transparent manner; the appearance of the application to the user

remains unchanged but the security is improved;
- insertion of authentications; is made to give rights only to the users that prove they are part of the system;
- data restrictions are used to protect the data the application works with from the bad intended users and from the users without access rights;
- updates only by adding information are made to protect the data from the attacks made by system's users;
- development of software components that cover better the vulnerabilities through the training of the developers and awareness of the most frequent risks.

Increasing the security of the applications above a certain level is justified only if the costs implied by its lack are higher than the costs for implementation.

3 Mobile Citizen Oriented Applications

Mobile citizen oriented applications are mobile clients for the citizen oriented informatics applications. These must comply with many restrictions of the mobile clients that they must run on:
- low bandwidth is a problem for the users that don't have an unlimited data plan or available wireless connection at their disposal;
- low memory is usually the case with mobile devices;
- limited processing power is another characteristic of the mobile devices;
- limited screen size is another issue to be taken into account at the development of the mobile citizen oriented applications;
- low and various screen resolution;
- the diversity of producers leads to a high diversity of operating systems for the mobile devices;
- user input problems are caused by the design of the devices.

There are many limitations of the mobile devices but the scope of the development team of the mobile citizen oriented application is to find solutions and approaches to deliver the user the desired content and solve his problem. Mobile technologies are in a continuous process of improvement as the mobile devices and mobile services market is expanding at a very large scale.

On the mobile devices the authentication services can be automated as most of the applications have access to some form of persistent storage in the memory of the device. Even of web forms, the browsers implement intelligent algorithms to detect password fields and store the username and password if the user desires so. The automatic authentication is a good feature considering that the owner of the device is the only one using the device. If the device is stolen, other persons can use the automatic authentication using the device, but the business devices that are the most sensible to data privacy offer technologies for the remote deletion of data so even if the device is stolen, the data is cleared by the owner. An alternative method of authentication requires the user to define a link between his identity/credentials and the IMEI of the device he is using on a regular basis. The IMEI can be automatically obtained by applications and, on the basis of this unique identification string, the application searches for associations with credentials and automates the authentication process. If more than one credential are associated with one IMEI, the user is allowed to select the desired one. In the mobile citizen oriented applications this is usually not the case as each user accesses its own account and doesn't need more than one account at a time. The authentication of the user can be transmitted between the applications so that the user doesn't need to authenticate on each application. This assumes that links are made between the different applications and the credentials users use for each one. The authentication problem is complex and sensitive and more and more techniques that make it both more secure and more easy to use by the users appear.

4 Authentication methods for citizen oriented mobile applications

According to [11] the application security represents the measures taken to prevent the exceptions in the security policy of an application or the vulnerabilities encountered through the application processes: design, development, deployment, upgrade and maintenance.

The security is a must that should be taken into account when designing any application, not only the ones for mobiles. For these, there should be done the application risks analysis.

Risk analysis creates an inventory and determines exposure to threats, the likelihood of producing and the impact on the application.

Risk approach provides ways of intercepting the risk and avoiding consequences [12]:

- *acceptance*; no special actions are taken to avoid consequences of producing a risk;
- *impact mitigation*; special measures are taken to provide reduced consequences of producing the risk;
- *transfer*; external components will deal with the producing of the risk;

According to [12], the security mechanisms must be transparent, in such a way they don’t interfere with the usability of the application and there should be a balance between the confidentiality, integrity and availability of the application.

According to [12] the underlying principles of security solutions are:

- *authentication* - the process of establishing a claimed identity; the initiator makes a request to a security component that you have to prove identity;
- *authorization* - the process of determining whether a validated entity has permission to access a secure resource based on attributes, conditions and circumstances;
- *integrity* - preventing change and destruction of property by an unauthorized entity, synonymous with data integrity;
- *availability* - protection from attacks such as denial of service;
- *confidentiality* - information is not disclosed to unauthorized entities;
- *independence* - business registration system at a level that ensures the production order reconstruction of events;
- *non-repudiation* - preventing the denial of the role of a participant in a transaction.

Regarding the client-server applications, the security issues are related to the fact that data travels between various components through a network. In the network data is transferred through intermediate nodes.

The types of security issues with communications include [12]:

- eavesdropping - the information is intercepted without changing the information itself;
- tampering – the information is modified and then sent further on to the recipient;
- impersonation – the information is passed from or to a person pretending to be someone else, or a person who misrepresents himself.

As cellular technology is evolving, supporting large amounts of data to be transferred, having improved connectivity, many network applications arise. The security threats become important for mobile applications as well.

An important aspect of security for mobile e-commerce communication is the ability to authenticate a message sender’s identity. Widespread are the public-key-infrastructure PKI [12] mechanisms. This consists of a set of technologies that rely on encryption and digital certificates. The certificates are message attachments, issued by an independent authority that authenticate sender’s identity and provide encryption keys. PKI works with public keys. The certificate issuer authority generates a pair of public/private keys. The public key is used to encrypt the message and the private key is used to decrypt it. The public key is available to people the sender communicates to and the private key is kept safely. Receivers that have access to the public key send encrypted messages back to the sender which is the only who can decrypt it.

Mobile devices have low computational power and such mechanisms are difficult to implement.

Other approaches make use of smartcards. PKI information is kept in smartcards that can be inserted into a device mounted reader.

Biometrics are also taken into account for mobile security. Unique physical characteristics are used to identify users.

All these security mechanisms use encryption algorithms. In order to implement any security mechanism it is necessary to exist the underlying foundation made up of tools, algorithms and programming support.

At device level, security is also important regarding the privilege a running application has over the device. If a Windows Mobile 6 device is taken into account then security features are assessed. Paper [13] presents all the security features included at device level and operating system level

In [14] the authentication represents the act of establishing or confirming the identity of a person, the degree of trusting for computers programs and delegation identity.

There are defined different types of authentications:

- the classic one, which is represented by the one using typed password
- fingerprint authentication
- voiceprint
- video authentication.

There are created different types of elements that are desired to assure a high degree of reliability, such as digital signatures, fingerprints, voice recognitions, video recognitions and passphrases in the content of the messages.

An electronic signature; public key infrastructure is often used to cryptographically guarantee that a message has been signed by the holder of a particular private key.

The applications which use the **password authentication** are represented by the ones where the user needs to introduce a password to access the information. This type of authentication refers to the form authentications, and has the following characteristics:

- it is easy to be implemented
- it is the most used authentication method, because the mobile device should only have the keywords
- it is a cheap method of authentication [15], because there it isn’t necessary to buy and install extra software.

The weaknesses of this authentication are the followings:

- even if there are used different cryptographic algorithms for stocking the users credentials, the others persons can see these dates, user and password when the user introduce them into the mobile device, so the security level depends also of the ability of every user in maintaining his own credentials secret.

The **fingerprint authentication** is a more secure method than the password authentication, because even if another user wants to use the mobile device, it can do so, because it will be necessary to put the fingerprint of the user, which is specific to every person.

This method of authentication is specific to PDA and consists on a fingerprint identification unit, which performs the entire authentication process and returns a score for verdict determination to the PDA [16]. The PDA capture the fingerprint when the user signs in for the first time and this became the comparison for the following fingerprints. The next time the user wants to sign in to application, he will pass another fingerprint which will be compared with the original one, and if these one are the same, the user will be authenticated.

In Figure 2 is presented the flowchart of fingerprint authentication.

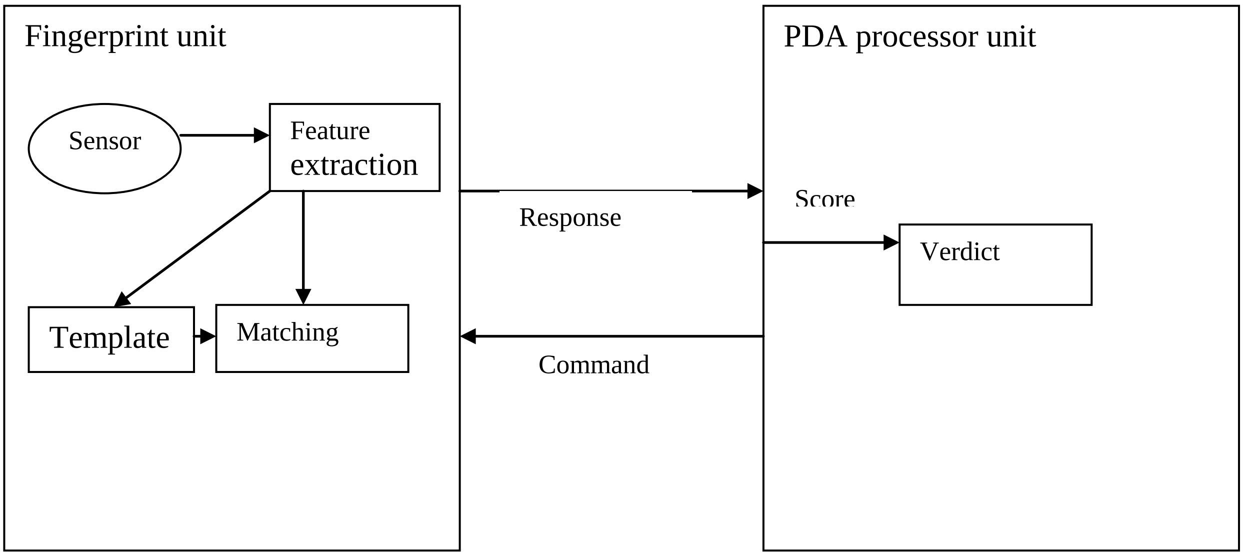


Fig. 2. Flowchart of fingerprint authentication

Fingerprint authentication has two main parts: enrollment and verification.

The fingerprint authentication advantages are:

- the speed of authentication process [17] there will take only a few seconds to authenticate a user
- because of the biometric characteristics, the information's cannot be copied so easily

The fingerprint disadvantages are [16]:

- it is expensive
- if the biometric information is compromised, it is extremely vulnerable
- biometric information can be mechanically copied and cannot be easily changed, but this is done only by the experts
- fake biometrics captured on different sticky tapes, but this is done only by the experts.

The fingerprint and voiceprint are biometrical ways of authentication. For many biometric identifiers, the actual biometric information is rendered into string or mathematic information [18]. The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data [18]. The comparison is made between two data strings, and if there is sufficient commonality the authentication is true. It may be appreciated that choice of how much data to match, and to what degree of accuracy, governs the accuracy/speed ratio of the biometric device. All biometric devices, do not provide unambiguous guarantees of identity, but rather probabilities and all may provide false positive and negative outputs [18].

Modern cell phones have various components to achieve more functionality. Sensors enlarge the range of applications. Accelerometer sensors are components that get device orientation and their main purpose is to help the operating system rotate the screen.

Its main characteristics are:

- The measurement range; accelerometers with output values ranging from -1g to 1g are limited for recording activity as they can only sense display orientation an d small movements on axes; accelerometers with output values ranging from more than 1g in absolute value may be used to detect gestures and shakes;
- The resolution; the more intermediate values between the minimum and maximum values, the more accurate is the difference between two similar movements;

The sampling rate; the sensor is able to collect acceleration values a number of times per second; some accelerometers are able to sample data at 120 Hz; however human motion while exercising has a periodicity between half a second to a few seconds; so, to gather information about the movement, a sampling frequency of 10-20Hz is enough.

A typical tri-axial accelerometer is a sensor that reports the acceleration of the device on the three axes derived from watching the phone screen in portrait mode as presented in figure XX:

- the positive x axis is from the center of the screen to the right of the screen
- the positive y axis is from the center to the top of the screen
- the positive z axis is from the center of the screen towards the viewer.

Figure 3 shows the conventional axes for mobile phone devices.

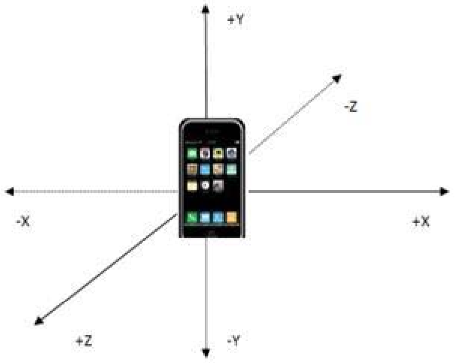


Fig. 3. Mobile phone coordinate system

The accelerometer always senses gravity. When moving the phone, by rotation, the gravity vector moves its components across the axes with different intensities, but the total acceleration is equal to the gravity. Holding the phone, the user performs gestures as sets of movements. Successive movements change the orientation of the device accordingly. If the movements are repeated in the same manner, the successive movements are interpreted as a code. If a user creates a personal unique gesture, this gesture is used to identify the user.

Research papers focus on these alternative ways of authenticating users such as the methods presented in [19] and [20].

An authentication method based on gestures is proposed. To authenticate to an existing application, the user has to perform a gesture with the phone, gesture that is recognized by the application and if it matches the previously enrolled gestures, the access to the resources is granted. This type of authentication is implemented using data collected from the accelerometer sensor.

The objective of implementing gesture based authentication is to grant easy access to applications.

The proposed method involves the following steps:

- password enrollment; the user shows the application the gesture used for authentication; the user provides several examples of the gesture, as no one can repeat the gesture exactly the same each time;
- training; a neural network component learns the patterns of the performed gesture;
- testing; the user authenticates providing again the gesture; the gesture is recognized and the access is granted; if the gesture is not recognized, then the attempt is rejected.

The proposed method uses a feed forward neural network to learn the patterns of the gesture using a back propagation algorithm. The architecture of the network consists of:

- the input layer; data is recorder for 5 seconds at 5 Hz sampling rate and each record contains 3 values for the X, Y and Z axis acceleration; the input layer consists of neurons for the whole ensemble of 75 values;
- the hidden layer; it consists of 25 units;
- the output layer; it consists of one unit; the output is 1 if the input matches the password or 0 if the input is different from the password;
- the activation function is sigmoid;
- the input values are real values in range [-16 m/s^2; 16 m/s^2] normalized to [-1,1]; the test accelerometer measures acceleration between [-1.6 g; 1.6 g].

Data collection is performed by recording 5 seconds of movement sampled at 5Hz. Graphically, the data for one example of correct password is presented in Figure 4.

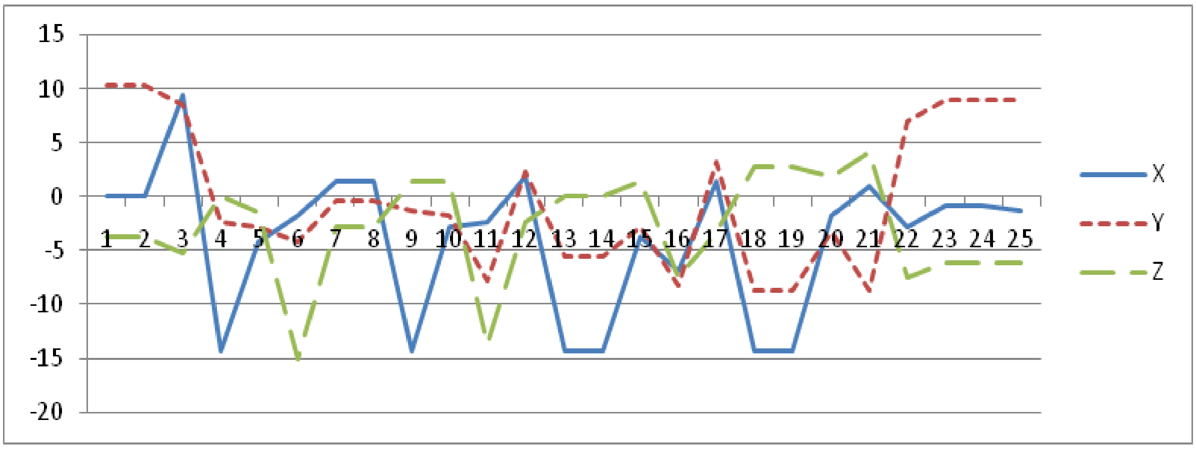


Fig. 4. Tri-axial accelerometer data for enrolled password

In Figure 5, there is presented the graphic information about the data collected for a successful login attempt.

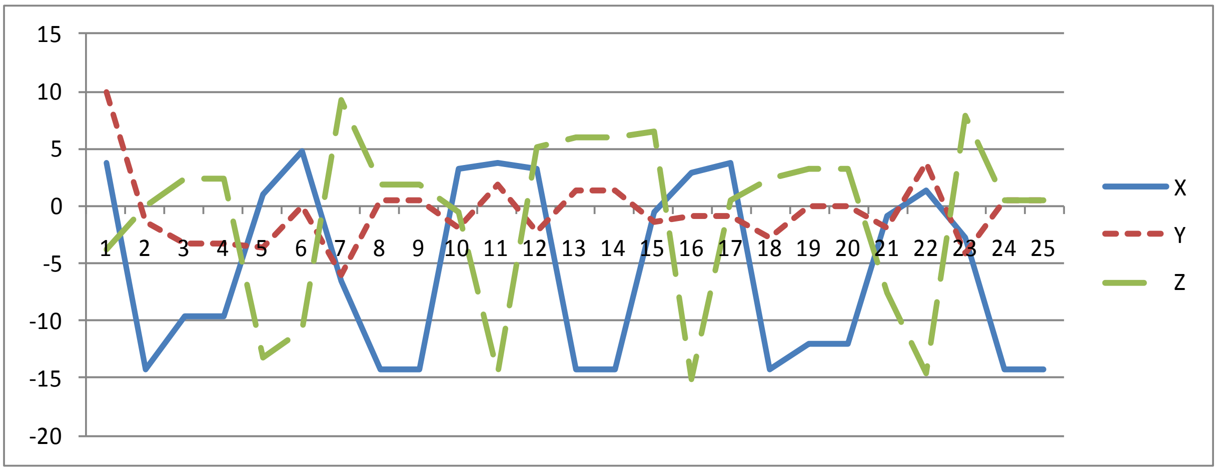


Fig. 5. Tri-axial accelerometer data for enrolled password for successful login attempt

It is observed from Figures 4 and 5 the obvious fact that a person cannot reproduce a gesture accurately. This makes necessary a measure that shows the similarity between recorded passwords and login attempts. In this research, simple statistical methods like correlation or histogram similarity were not very accurate. This is the reason a neural network was used. The neural network has the ability to learn given examples and further is able to generalize rules and give correct outputs for similar but not identical inputs.

In order to assess the quality of the approach it terms of ease of use, an indicator is built:

$$I_S = \frac{NS}{NT}$$

where

I_S – the indicator showing the rate of successful authentication attempts

NS – the number of successful authentication attempts

NT – the total number of authentication attempts.

It is considered that the attempt is successful if for a given input gesture, the network outputs a value greater or equal to 0.85. Also there must be ensured that other gestures do not produce a positive from the authentication component.

In the test performed during the research, the I_S indicator reached a value of 0.75 meaning that 75% of authentication attempts were successful when using the right gesture.

The I_S indicator has a level influenced by:

- the complexity of the gesture; if the gesture is too complex, then it is difficult even for the user to reproduce it alike;
- the quality of network training; the network is trained to learn several pairs of given inputs and expected outputs; the process iterates until the error of the network falls under a threshold;
- the quality of the training set; the training set contains versions of how the user makes the gesture that allows him to access the application; the user has to keep the same manner in executing the gesture after training the application.

For a large group of users U_1, U_2, …, U_n, validation of the proposed method is done using an indicator

$$I_V = \frac{\sum_{i=1}^{n} I_{Si}}{n}$$

where

I_V – the validation indicator;

I_{Si} – the success rate for user U_i.

If the value of I_V is greater than 0.85, then the method is validated for the considered group of users. If the group of users is representative for the collectivity of users that use a certain application using gesture based authentication, then the method is validated in general.

The robustness of the authentication method resides in the fact gestures have many peculiarities in execution for different individuals. Also, the information about the enrolled passwords is encapsulated in the neural network and cannot be retrieved as it is not kept in clear, but only weights between neurons create a model for input classification.

The performance of the approach is given by the performance of the neural network. The neural network takes around 28 seconds to train on a Windows Mobile 6.5 device with a 528 MHz processor in an implementation written in C# .NET. After training, the network is saved in a file. When applying inputs to the network, the outputs are very rapidly obtained with no perceivable delay for the user.

Gesture based authentication must be followed by alternative methods such the classic method with username and password. If the user has difficulty in logging in the he must be able to recover its rights to access the application.

5 Conclusions

Citizen oriented applications appeared to deliver a high degree of satisfaction to the final user. These are created to solve the citizens’ problems, not the problems of the owner of the application. The citizen oriented applications, due to their specific goal, differ from the traditional with many aspects. There are also many application structures that these applications can use. The development cycle is also modified when compared with the development cycle of the traditional distributed applications. The target group is analyzed very well so all requirements are captured and implemented by the applications. Each step of the development cycle has citizen-specific modifications that overall lead to the desired citizen oriented application. The security of the citizen oriented applications is vital. The security requirements are given by some of the attributes of the citizen oriented applications. There are also some vulnerabilities specific to the citizen oriented applications. All these must be addressed in order to obtain applications that deliver users a high level of satisfaction. There are many ways of increasing the security. All of them increase the complexity of the applications. The mobile citizen oriented applications are mobile clients for the server modules. These are designed to run on mobile devices such as mobile phones, smartphones, PDAs. There are many restrictions that the applications must respect in order to be able to run on mobile devices. The most important are: screen size and resolution, limited resources and limited user input. The automation of the authentication processes is a satisfying process for the user that doesn’t have many drawbacks. Different approaches for the automation of the authentication process exist and new ones are developed due to the development in mobile technologies.

Nonstandard authentication methods aim to be easy to use and do not require a lot of effort to apply. Accelerometer sensors permit the implementation of gesture based authentication. Gesture based authentication is easy to use and relatively easy to implement. It must be validated by a large number of users before becoming a standard type. When using gesture based authentication, also other methods of authentication must be available in parallel.

Acknowledgements

This article is a result of the project „Doctoral Program and PhD Students in the education research and innovation triangle". This project is co funded by European Social Fund through The Sectorial Operational Program for Human Resources Development 2007-2013, coordinated by The Bucharest Academy of Economic Studies.

References

[1] I. Ivan, B. Vintila, and D. Palaghita, "Types of Citizen Oriented Informatics Applications," *Open Education Journal*, no. 6, 2009.

[2] C. Y. Yoon, "Measures of perceived end-user computing competency in an organizational computing environment," *Knowledge-Based Systems*, vol. 22, no. 6, pp. 471-476, Aug. 2009.

[3] I. Ivan, B. Vintila, C. Ciurea, and M. Doinea, "The Modern Developments Cycle of Citizen Oriented Applications," *Studies in Informatics and Control*, vol. 18, no. 3, 2009.

[4] F. O. Bjørnson and T. Dingsøyr, "Knowledge management in software engineering: A systematic review of studied concepts, findings and research methods used," *Information and Software Technology*, vol. 50, no. 11, pp. 1055-1068, Oct. 2008.

[5] S. Liu, "Integrating top-down and scenario-based methods for constructing software specifications," *Information and Software Technology*, vol. 51, no. 11, pp. 1565-1572, Nov. 2009.

[6] P. Pocatilu, *Costurile testarii software*. Bucharest, Romania: ASE Publishing House, 2004.

[7] B. L. Vinz and L. H. Etzkorn, "Improving program comprehension by combining code understanding with comment understanding ," *Knowledge-Based Systems*, vol. 21, no. 8, pp. 813-825, Dec. 2008.

[8] D. Mellado, E. Fernández-Medina, and M. Piattini, "Towards security requirements management for software product lines: A security domain requirements engineering process ," *Computer Standards & Interfaces*, vol. 30, no. 6, pp. 361-371, Aug. 2008.

[9] D. Palaghita and B. Vintila, "Security Risk Analysis Using Citizen Oriented Applications," in *Ninth International Conference on Informatics in Economics*, Bucharest, 2009.

[10] D. Palaghita, "The Post-Release Lifecycle Security Costs of Open Source Products," *Open Source Science Journal*, vol. 2, no. 1, pp. 56-71, 2010.

[11] Microsoft Patterns and Practices. (2010, May) Improving Web Application Security:Threats and Countermeasures. [Online]. http://msdn.microsoft.com/en-us/library/ms994920.aspx

[12] A. Visoiu and S. Trif, "Open Source Security Components for Mobile Applications," *Open Source Science Journal*, vol. 2, no. 2, pp. 155-166, 2010.

[13] Microsoft. (2010, May) Security Model for Windows Mobile 5.0 and Windows Mobile 6. [Online]. http://technet.microsoft.com/en-us/library/cc182298.aspx

[14] Federal Financial Institutions Examination Council. (2010, Jun.) Authentication in an Internet Banking Environment. [Online]. http://www.ffiec.gov/pdf/authentication_guidance.pdf

[15] T. IIA. (2010, Jun.) Advantages and disadvantages of different authentication tools. [Online]. http://www.theiia.org/download.cfm?file=29264

[16] W. Jansen, R. Daniellou, and N. Cilleros. (2010, May) Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation.

[17] M. Vaclav and R. Zdenek. (2010, May) Biometric authentication - security and usability. [Online].

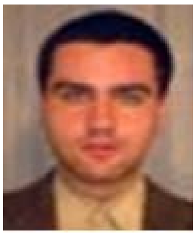
http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

[18] GPayments. (2010, Jun.) Two-factor authentication An essential guide in the fight against Internet fraud. [Online]. http://www.gpayments.com/pdfs/WHITEPAPER_2FA-Fighting_Internet_Fraud.pdf

[19] R. Mayrhfer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *Proc. Pervasive 2007: 5th International Conference on Pervasive Computing*, vol. 4480, 2007, pp. 144-161.

[20] D. Gafurov, K. Helkala, and T. Sondrol, "Biometric Gait Authentication Using Accelerometer Sensor," *Journal of Computers*, vol. 1, no. 7, pp. 51-59, Nov. 2006.

Ion IVAN has graduated the Faculty of Economic Computation and Economic Cybernetics in 1970. He holds a PhD diploma in Economics from 1978 and he had gone through all didactic positions since 1970 when he joined the staff of the Bucharest Academy of Economic Studies, teaching assistant in 1970, senior lecturer in 1978, assistant professor in 1991 and full professor in 1993. Currently he is full Professor of Economic Informatics within the Department of Computer Science in Economics at Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies. He is the author of more than 25 books and over 75 journal articles in the field of software quality management, software metrics and informatics audit. His work focuses on the analysis of quality of software applications.



Adrian VISOIU graduated the Bucharest Academy of Economic Studies, the Faculty of Cybernetics, Statistics and Economic Informatics. He has a master degree in Project Management. He is an assistant lecturer in the Economic Informatics Department of the Bucharest Academy of Economic Studies. He published 16 articles alone or in collaboration and he is coauthor of three books. His interests include: object oriented programming, data structures, multimedia programming, software quality management, software metrics refinement.

Silvia TRIF graduated the Faculty of Cybernetics, Statistics and Economic Informatics. She has a Master’s Degree in Project Management. Her interests are mobile applications, information security and project management.

Bogdan VINTILĂ graduated the Bucharest University of Economics, the Faculty of Cybernetics, Statistics and Economic Informatics. He is currently a PhD candidate in the field of Economic Informatics at University of Economics and at the University of Gothenburg in the Applied IT department. He is interested in citizen oriented informatics applications, developing applications with large number of users and large data volumes, e-government, e-business, project management, applications' security and applications' quality characteristics.

Dragos PALAGHITA graduated from the Academy of Economic Studies of Bucharest, Cybernetics Statistics and Economic Informatics faculty, Economic Informatics section in 2008. He is programming in C++ and C# and his main areas of interest are Informatics Security, Software Quality Management, large data set analysis and graphical representation enchancements. Currently he is undergoing PhD studies at the Academy of Economic Studies of Bucharest.