Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 62 (2015) 547 – 554

Procedia
Computer Science

The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

Exploring a Context-based Network Access Control for Mobile Devices

Yaser Mowafi[a,*], Dhiah el Diehn I. Abou-Tair[a], Ahmad Zmily[a], Tareq Al-Aqarbeh[a], Marat Abilov[b], Viktor Dmitriyevr[b]

[a]*School of Information Technology and Engineering, German-Jordanian University, 11180 Amman, Jordan*
[b]*Carl von Ossietzky University, Department of Computing Science, 26111 Oldenburg, Germany*

Abstract

Significant advancement in mobile devices coupled with high speed networks have shifted personal computing towards pervasive environments. Mobile devices currently offer many value-added applications and services such as emailing, messaging, navigation, social networking, finance, and entertainment. Typically, such value-added applications have access to users' personal information and are capable of gathering and transmitting trust sensitive information, hence posing security risks and/or privacy concerns. In this paper, we propose a context-based analytic hierarchy process (AHP) framework for eliciting context information and adapting this information with network access control measures for mobile devices. The framework enforces the execution of mobile applications inside security incubators to control the communication between mobile applications and mobile device resources. Mobile applications' access requests are analyzed based on user's context information collected from the mobile device sensors and the application network access control configuration. We use the Facebook mobile application, as a test case, to evaluate our proposed framework. Evaluation results have demonstrated the efficacy of the framework in providing network access control measures based on real-time assessment of user's context.

Peer-review under responsibility of organizing committee of The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

Keywords: Mobile Computing; Context-aware Computing; Analytic Hierarchy Process; Multi-criteria Decision Making; Agent System

1. Introduction

Significant advancements in mobile device technologies have shifted personal computing to pervasive and ubiquitous environments. Today, smart phones, in addition to making regular calls, are widely used for reading emails, text messaging, documents viewing, mapping, surfing the web as well as for entertainment purposes such as watching movies, listening to music, playing games, etc. Today's smart phones are equipped with various built-in sensors that are capable of collecting and providing high precision and accurate data, such as location, motion, acceleration, rotation, and environmental conditions like temperature, pressure, and illumination. These mobile devices use the

[*] Corresponding author. Tel.: +962 6 429 4133 ; fax: +962 6 429 4133.
E-mail address: yaser.mowafi@gju.edu.jo

Peer-review under responsibility of organizing committee of The 2015 International Conference on Soft Computing and Software Engineering
(SCSE 2015)
doi:10.1016/j.procs.2015.08.530

collected data to smartly recognize and interpret their surrounding environment. Applications can then use that information to adapt their interfaces or to react according to the inferred context. For example, a mobile phone may sense nearby Bluetooth-enabled mobile devices within its range and enable users to exchange and share information to facilitate a social interaction[1]. Such value-added applications and services typically require collecting not only users' personal information, such as location or identification, but also gathering and transmitting trust sensitive information.

Mobile applications typically have no restrictions on collecting users' preferences either directly through user solicitation, or indirectly through explicit or implicit user feedback. This unrestricted access possess a threat to users' security and privacy. In addition, some applications with malice aforethought may use some of the applications on the users' mobile device to execute trust sensitive information. Although many mobile applications typically provide security mechanisms to protect users' information from such malicious attacks and/or intrusion, however application should not be solo trusted with protecting users' security and privacy.

Information security structure for smart phones should be neither static nor application-centric. Instead, the need is for a context-aware adaptive system that applies context information to improve security decisions for different situations and users actions. The system, in addition to require user inputs, has to proactively change security settings as users' context changes. For example, using the smart phone to initialize a payment transaction should require higher security measures than using the phone to take a photo.

In order to address the above challenges with mobile devices, we propose a context-based adaptive framework for eliciting context information and adapting this information with network access control measures. The framework consists of multi-security incubators, in each of which, a mobile application can be executed. The incubator, or sandbox, controls the communication between the mobile application and the mobile device resources. Executing each application within its own incubator as a standalone application makes it possible to control the communication mechanism within the incubator. Hence, there will be no need to make any changes to the application itself. To illustrate the effectiveness of our proposed framework, we validate it for the Facebook application using Google's Nexus smart phone running Android Operating System (OS).

2. Related Work

Jakobsson et al.[2] develop an implicit authentication model using observed user behavior such as motion, phone activity etc. to authenticate users' access to their mobile devices. Conti et. al.[3] propose CRePE framework to enforce access policies based on predefined context-related policies that are set by the users. Garcia-Morchon and Wehrle[4] extend traditional Role Based Access Control (RBAC) systems in critical, emergency, and normal access control situations, using modular access control policies running on resource-constrained sensor nodes. Di Cerbo et al.[5] propose a prototype, called ProtectMe, that exploits "Sticky Policies" (SP) attached to resources and prescribed usage conditions. ProtectMe integrates SPs with mobile devices, and dynamically enforces their constraints. Khan and Sakamura[6] explore the relationship between security and context for ubiquitous services. They propose a context-aware access control model for ubiquitous healthcare services. Hayashi et al.[7] present a probabilistic model for context-aware scalable authentication in order to enable the selection of appropriate active authentication factors given a set of passive authentication factors. Filho and Martin[8] propose an owner-centric QoC-Aware Context-Based Access Control model that takes into account both context information and its QoC indicators to grant and to adapt access permissions to resources. Chakraborty et al.[9] introduce a context-aware model-based solution to prevent privacy in mobile application. The desired framework uses current user context together with a model of user behavior to quantify an adversary's knowledge regarding a sensitive inference, and obfuscate data accordingly before sharing.

Of the most related efforts to this work, Fischer and Karsch[10] propose an ontology-based framework that utilizes context information (i.e., locations: home, office; activity: meeting, travelling) to derive security access measures of the mobile devices assets, such as messages, based on the confidentiality level of these assets. Similarly, Johnson et al.[11] deploy annotated programming approach that incorporates context information for security access control of different types of objects (i.e., least important, somewhat important and very important) and different types of access operations (i.e., read only, append, or read and write). Gupta et al.[12] propose a context profiling framework using location WiFi and Bluetooth to infer appropriate access and sharing policies for sensitive data on the device.

Table 1: Context aspect and their states

Context Aspects	1	2	3	4	5	6
Location	Undefined	Home	Work	Public		
Time	Morning	Forenoon	Noon	Afternoon	Evening	Night
Speed	Still	Low	Medium	High		
Network	Undefined	Home WLan	Work WLan	GSM	Public hotspot	
Noise	Silence	Low	Medium	High		
Light	Darkness	Low	Medium	High		

3. Context-based Network Access Control Model

The proposed framework consists of mobile application sandbox and context shadow application. The mobile application sandbox is built inside the mobile OS. The sandbox incubates mobile applications data and code execution, and also conceals the network access from the mobile application. This means that the application can access the network only through the sandbox. To avoid any changes to mobile OS, the network access control component will be implemented as a shadow application.

When the running mobile application attempts to get a network access, the application sends TCP SYN request as a part TCP handshake. This attempt triggers a network access security checking method in the sandbox which is forwarded to the shadow application. The shadow application analyzes the request considering the network access security level and responds with allow or reject, which is applied to the request in the sandbox. The network access security level is defined based on both the user's context information collected from mobile device sensors and the application configuration. The security configuration comprises of the following: Black (deny) or white (allow) list of context aspect values; Importance factors for each context aspect values.

Context aspect values will be assigned a categorical values as illustrated in table 1.

The application consists of the following components: application component, which is the main component that manages all requests from the sandbox and provides the network access control decision; factorProcessor component, which processes the importance factors of context aspects using AHP method, that will be presented in the next section; context component, which gathers and categorizes the context information.

When the shadow application receives an access request from the sandbox, it activates the Controller object. The Controller object loads the application configuration and initializes new Application object with these settings. The Controller object then forwards the request to the Application object. The Application object requests from the Context object an update of the context aspect values. The Application object uses the Rule object to evaluate the context aspect values and the application configuration to make the appropriate decision. This decision will then be returned to the sandbox.

4. Analytical Hierarchy Process

Context entails a variety of aspects that are dynamically combined together to create a certain context. While some of these aspects are tangible and objectively measured (e.g., time, speed, and noise), others are intangible and subjectively measured (e.g., place and proximity). As each context aspect contributes a certain portion to the overall context value, therefore from a decision making perspective it will be necessary to consolidate these context aspects into a single integrated decision problem[13]. Such consolidation allows for establishing a multi-criteria decision making (MCDM) problem that links between the various context aspects, of which their relative attribute to the overall context are derived. A popular methodology for dealing with MCDM problems is Analytic Hierarchy Process (AHP) method[14,15]. Compared to other MCDM problem methods, AHP has the advantage of handling both tangible and intangible criteria that entails a systematic procedure in the thought process[15].

AHP has been widely used in a variety of policy selection, decision making, adaptive learning, recommendation and feedback systems. For example,[16] use AHP for personalized learning mechanism recommendation depending on the user's learning task. Others[17] apply AHP in determining mobile devices notification service prioritization based on user's awareness of incoming calls and appropriation preferences. Lastly,[18] utilize AHP-based mechanism

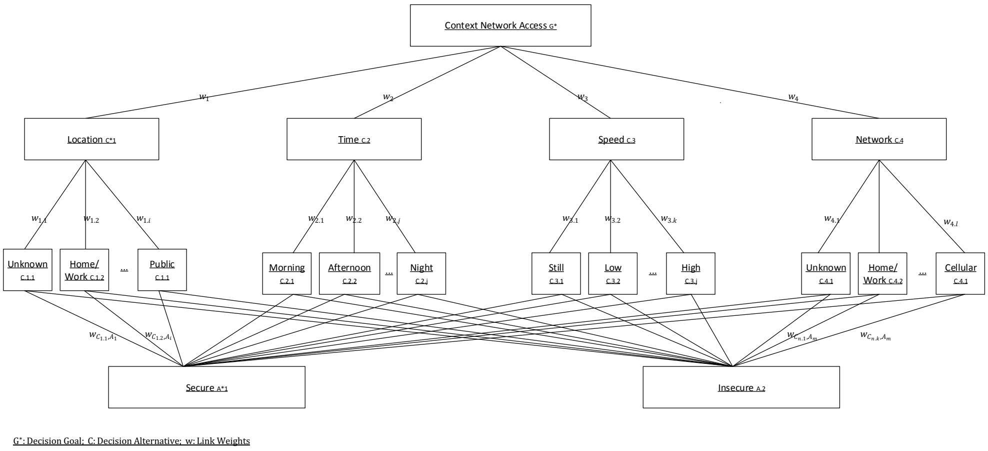


Fig. 1: An AHP Hierarchy Structure

to develop a web-based recommendation system that can help in selecting proper mobile phone models based on users' preference of phone hardware features and functions.

When applied in decision problems, AHP assists to describe a general decision operation by decomposing the decision problem into a multi-level hierarchic structure. As shown in Figure 1, the top of the hierarchy represents the problem decision goal; the bottom denotes the decision problem alternatives $A_1 \cdots A_i$; and the decision criteria C_i and Sub-criteria $C_{i,j}$ are in the middle level. The lines connecting the criteria and the decision goal at the one hand, and the lines that link the decision criteria with the alternatives at the other hand represent the AHP decision tree. The link weights ω_i and $\omega_{i,j}$ are determined through a pairwise comparison of C_i and C_i, j, respectively. In the figure, $\omega C_{i,j}, A_i$ is the score of alternative A_i with respect to criterion $C_{i,j}$ and $\omega_{i,j} X \omega C_{i,j}, A_i$ is the portion of the score that the specific criterion receives in the overall evaluation of the competing components. The relative weight value of the alternatives can be determined by calculating and then consolidating the weighted values of the decision criteria components. The general process of the AHP analysis of a decision problem includes the following:

Step 1: Create a hierarchical structure that represents the key elements of the decision problem. The top level of the hierarchy represents the overall objective, or the decision goal. The second level includes the relevant criteria and sub-criteria of the decision problem and the third level represents the decision alternatives.

Step 2: Utilizing the pair-wise comparisons, AHP applies an eigenvalue method to determine a ranking weight for criterion and its sub criteria variables using a pair-wise comparison among each alternative. For example, a pair-wise comparison of q elements' weights, $\omega_1, \omega_2, \cdots \omega_q$ is performed via composing the following comparison matrix.

$$\begin{pmatrix} \frac{\omega_1}{\omega_1} & \frac{\omega_1}{\omega_2} & \frac{\omega_1}{\omega_3} & \cdots & \frac{\omega_1}{\omega_q} \\ \frac{\omega_2}{\omega_1} & \frac{\omega_2}{\omega_2} & \frac{\omega_2}{\omega_3} & \cdots & \frac{\omega_2}{\omega_q} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \frac{\omega_q}{\omega_1} & \frac{\omega_q}{\omega_2} & \frac{\omega_q}{\omega_3} & \cdots & \frac{\omega_q}{\omega_q} \end{pmatrix}$$

In this matrix, every element a_{ij} of each trial is the result of a paired comparison denoting the dominance of element $_i$ relative to element $_j$. A comparison is also being made of the $_jth$ element with the $_ith$ element. This results in the comparison matrix being a reciprocal matrix satisfying $a_{ij} = l/a_{ij}$. The matrix diagonal represents the self comparisons on the matrix elements. To associate the overall weighting for each element relative to the level immediately above it, a so called priority vector (PV), which represents the eigenvector of the paired comparison matrices' components. The priorities assigned to the matrix elements reflect the order of their importance with respect to each alternative.

Step 3: Consolidate the weighted values in the earlier step, using the eigenvectors of the hierarchy alternatives to create an overall priority value for each alternative relative to the overall decision problem goal.

Table 2: Priorities for security alternatives with respect to the Location context aspect states

Location-Undefined	Allow	Deny	Priority		Location-Home	Allow	Deny	Priority
Allow	1	1/9	0.1		Allow	1	9	0.9
Deny	9	1	0.9		Deny	1/9	1	0.1
Location-Work	Allow	Deny	Priority		Location-Public	Allow	Deny	Priority
Allow	1	7	0.875		Allow	1	3	0.75
Deny	1/7	1	0.125		Deny	1/3	1	0.25

Table 3: Pairwise comparison of context aspects

Context Aspect	Location	Network	Time	Noise	Light	Speed	Priority
Location	1	1/3	5	7	7	7	0.29
Network	3	1	7	9	9	9	0.50
Time	1/5	1/7	1	3	3	3	0.09
Noise	1/7	1/9	1/3	1	1	1	0.04
Light	1/7	1/9	1/3	1	1	1	0.04
Speed	1/7	1/9	1/3	1	1	1	0.04

We deploy AHP method to determine the relative weights of the context-based network access control alternatives (deny access, allow access). This is performed through a paired comparison among the context aspects criteria (i.e., location, time, speed, light, and noise) towards achieving context value.

5. Case Scenario

We have implemented our proposed context-based network access control framework described in Section 4 for the Google Android platform. The proposed solution features a small overhead in terms of time and computation energy requirements, thus supporting the feasibility of the framework implementation on mobile devices. We have selected the Facebook mobile application to illustrate the network access control decision mechanism in the framework. Six different context aspects that are currently supported in many smart phones were selected. Table 1 shows the selected context aspects. Each context aspect can have up to six different states. For example, Location has four different states: Undefined, Home, Work, and Public, while Time has six states: Morning, Forenoon, Noon, Afternoon, Evening, and Night. The user is required to prioritize the context aspects according to his or her preferences. For example, the user can rank the different states for context aspect Location and specify a security level for each Location state. A possible rank is: Home, Work, Public, Unidentified; where Home has the highest security level and Unidentified has the lowest. When the Facebook mobile application is launched and attempts to get a network access, it triggers a checking request in the sandbox. The request is analyzed utilizing AHP method. The alternatives (Allow, Deny) priorities are calculated with respect to the context aspects (Location, Network, Time, Speed, Noise, and Light). First, a pair-wise comparison of context aspects is performed based on the user's preferences. The weaker alternative with respect to the context aspect is given a weight of 1. Using a scale from 1 to 9, the other alternative is assigned a weight with respect to the weaker alternative. Table 2 shows the AHP matrix and the priorities for each alternative with respect to the different states of the Location context aspect. Note that similar analysis is performed for the rest of the context aspects.

Next we evaluate the context aspects with respect to their importance in reaching the security level goal. Similarly, this is done by a series of pair-wise comparisons among the context aspects. The results of the pair-wise comparisons are placed in a comparison matrix as explained in Section 4. The priority of each context aspect in reaching the security level goal is calculated using AHP method. Table 3 shows the relative weights for the various pairs of context aspects and their priorities. When the user activates a functionality of the Facebook application, a request is triggered to access the network. At this point, the sandbox catches the request and forwards it to the shadow application. The

Table 4: An example of a current users context for an Allow network access desision

Context Aspect	State	A - Allow Alternative weight	B - Context Aspect Weight	A*B
Location	Work	0.88	0.29	0.25
Network	Work WiFi	0.83	0.50	0.42
Time	Evening	0.13	0.09	0.01
Noise	Low	0.88	0.04	0.04
Light	Darkness	0.88	0.04	0.04
Speed	Low	0.88	0.04	0.04
Overall relative weight of the Allow Alternative:				0.79

Table 5: An example of a current users context for an Deny network access desision

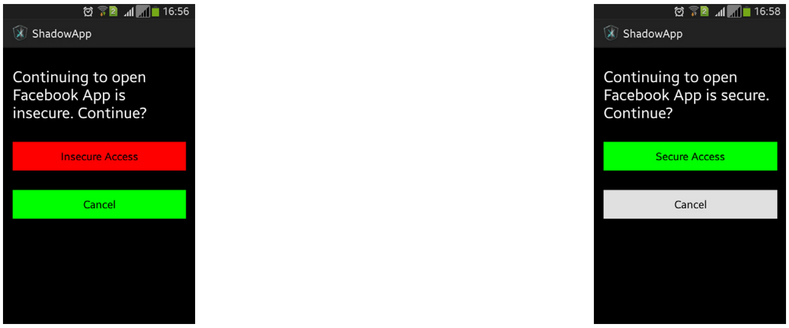
Context Aspect	State	A - Allow Alternative weight	B - Context Aspect Weight	A*B
Location	Public	0.75	0.29	0.22
Network	Undifined	0.10	0.50	0.05
Time	Forenoon	0.88	0.09	0.08
Noise	Low	0.88	0.04	0.04
Light	Medium	0.50	0.04	0.02
Speed	Still	0.90	0.04	0.04
Overall relative weight of the Allow Alternative:				0.44

shadow application uses the relative alternative weights and the context aspect weights of the current user's context to calculate the network access control decision value.

Table 5 shows an example for a user current context while using the Facebook application. The users location is at work. Note that Location-Work from Table 2 has a relative weight of 0.88 towards the Allow access alternative. Location context aspect (Table 3) has a relative weight of 0.29 towards the decision goal. The overall weight of the context aspect Location towards the Allow alternative is obtained by multiplying the two weights together which results into 0.25. Similar calculations are done for the rest of the context aspects. The overall relative weight of the Allow access alternative is calculated by summing the weights for all of the context aspects resulting in a relative weight of 0.79. The shadow application responds back to the sandbox with an Allow access whenever the calculated relative weight is above 0.50. In this case, a 0.79 relative weight results in an Allow access response Table 4 shows another example for the same user in a different context while using the Facebook application. In this context, Location is Public, Network is Undefined, Time is Forenoon, Noise is Low, Light is Medium, and Speed is Still. The shadow application recalculates the overall relative weight of the Allow access alternative resulting in a relative weight of 0.44. As this weight is below than the required 0.50 threshold of Allow access, therefore, the shadow application responds back to the sandbox with a Deny access.

6. PROTOTYPE IMPLEMENTATION

We developed a prototype application of our proposed network access control mechanism in Android OS on mobile devices. The prototype architecture extends the programmable features built in Android OS through the definition and implementation of control components that aim to equip the mobile device with context-based network access control features in run-time. The application enforces the execution of mobile applications inside the shadow application that controls the network access of these applications. As a use case, we select Facebook mobile application to implement and validate the network access control mechanism lifecycle. In our implementation, we incorporate four different context aspects (Fig. 1), currently retrieved in most current existing Android smart phones. For example, Network context aspect can have the following states: Unknown, Known network connection (i.e., Home Wi-Fi or Work Wi-Fi network), and Cellular network. The algorithm uses the instantaneous measures of the context aspect to estimate the network access security risk level of either low (GREEN) or high (RED). The security threshold corresponds to the calculated AHP value with respect to the context aspects relative weights (location, network type, time, and speed) and



Continuing to open Facebook App is insecure. Continue?

Continuing to open Facebook App is secure. Continue?

(a) Insecure Network Access

(b) Secure Network Access

Fig. 2: Screenshots of the shadow application network access screen

the relative weights of their corresponding current states. For example, Fig. 2a shows a network access attempt that is triggered with the launching of Facebook mobile application via our shadow application. In this context, the user location is determined to be Public, Wi-Fi network type is Unknown, time is Afternoon, and speed is Still. The shadow application calculates the overall relative weight of the context level using the AHP method. A relative weight below the fiftieth percentile threshold, in this case, yields a high security risk level (RED) that highly recommends the user not to continue with opening the Facebook application. Alternatively, Fig. 2b illustrates another scenario of a network access attempt of launching Facebook application, through our shadow application. In this case, the user's location is determined to be at Work, network type is a Work Wi-Fi, time is Evening, and speed is Low. The shadow application recalculation of the overall relative weight of the context level yields a relative weight above the fiftieth percentile threshold that yields a low security risk level (GREEN). Hence, prompting the user to continue with launching the Facebook application. In order to examine our proposed framework, we used the general cross-validation evaluation technique to test the power of accuracy of the network access alternatives and their associated context aspects. The validation of our framework draws on a dataset of five undergraduate university students affiliated participants (3 males and 2 females). Participants' age ranged from 18 to 21 years old with a mean age of 19. The participants are frequent mobile devices users, own Android mobile devices, and considered themselves as frequent users of mobile applications. Participants were then instructed to launch their Facebook application at various times and places over a week time period. The application logs this information, along with participants feedback options of whether they think that the network access is secure or not - relevant to the shadow application network access recommendation. The collected data resulted into approximately 200 observations of launching attempts of Facebook via the shadow application framework. The collected data were divided into 80% of training data, and the remaining 20% for testing. The results showed a classification accuracy of 91% with an average Euclidian distance of 0.008. Euclidian distance ranges from 0 for the perfect classifier and square root of two for incorrect classification.

7. Conclusions

In this paper, we propose a context-based network access control framework that incorporates user's context, collected from mobile device sensors, with network access control decisions. The framework applies AHP structured method for dynamically evaluating user's context, and provides the appropriate decision. We use the Facebook mobile application, as a test implementation case, to evaluate our proposed framework and method. The results have demonstrated the efficacy of our framework in enforcing network access decisions based on real-time assessment of user's context.

Acknowledgements

The work of this paper has been partially funded by the German Research Foundation (DFG) contract no. MA 328612-1.

References

1. Persson, P., Jung, Y.. Nokia sensor: from research to product. In: *Proceedings of the 2005 conference on Designing for User eXperience*; DUX '05. New York, NY, USA: AIGA: American Institute of Graphic Arts. ISBN 1-59593-250-X; 2005, URL: `http://dl.acm.org/citation.cfm?id=1138235.1138297`.
2. Jakobsson, M., Shi, E., Golle, P., Chow, R.. Implicit authentication for mobile devices. In: *Proceedings of the 4th USENIX conference on Hot topics in security*; HotSec'09. Berkeley, CA, USA: USENIX Association; 2009, p. 9–9. URL: `http://dl.acm.org/citation.cfm?id=1855628.1855637`.
3. Conti, M., Nguyen, V., Crispo, B.. Crepe: Context-related policy enforcement for android. In: Burmester, M., Tsudik, G., Magliveras, S., Ili, I., editors. *Information Security*; vol. 6531 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg; 2011, p. 331–345. URL: `http://dx.doi.org/10.1007/978-3-642-18178-8_29`. doi:`10.1007/978-3-642-18178-8_29`.
4. Garcia-Morchon, O., Wehrle, K.. Modular context-aware access control for medical sensor networks. In: *Proceedings of the 15th ACM symposium on Access control models and technologies*; SACMAT '10. New York, NY, USA: ACM. ISBN 978-1-4503-0049-0; 2010, p. 129–138. URL: `http://doi.acm.org/10.1145/1809842.1809864`. doi:`10.1145/1809842.1809864`.
5. Di Cerbo, F., Trabelsi, S., Steingruber, T., Dodero, G., Bezzi, M.. Sticky policies for mobile devices. In: *Proceedings of the 18th ACM symposium on Access control models and technologies*; SACMAT '13. New York, NY, USA: ACM. ISBN 978-1-4503-1950-8; 2013, p. 257–260. URL: `http://doi.acm.org/10.1145/2462410.2462429`. doi:`10.1145/2462410.2462429`.
6. Khan, M.F.F., Sakamura, K.. Context-awareness: exploring the imperative shared context of security and ubiquitous computing. In: *Proceedings of the 14th International Conference on Information Integration and Web-based Applications &#38; Services*; IIWAS '12. New York, NY, USA: ACM. ISBN 978-1-4503-1306-3; 2012, p. 101–110. URL: `http://doi.acm.org/10.1145/2428736.2428755`. doi:`10.1145/2428736.2428755`.
7. Hayashi, E., Das, S., Amini, S., Hong, J., Oakley, I.. Casa: context-aware scalable authentication. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*; SOUPS '13. New York, NY, USA: ACM. ISBN 978-1-4503-2319-2; 2013, p. 3:1–3:10. URL: `http://doi.acm.org/10.1145/2501604.2501607`. doi:`10.1145/2501604.2501607`.
8. Filho, J.B., Martin, H.. Qacbac: an owner-centric qoc-aware context-based access control model for pervasive environments. In: *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*; SPRINGL '08. New York, NY, USA: ACM. ISBN 978-1-60558-324-2; 2008, p. 30–38. URL: `http://doi.acm.org/10.1145/1503402.1503409`. doi:`10.1145/1503402.1503409`.
9. Chakraborty, S., Raghavan, K.R., Johnson, M.P., Srivastava, M.B.. A framework for context-aware privacy of sensor data on mobile systems. In: *Proceedings of the 14th Workshop on Mobile Computing Systems and Applications*; HotMobile '13. New York, NY, USA: ACM. ISBN 978-1-4503-1421-3; 2013, p. 11:1–11:6. URL: `http://doi.acm.org/10.1145/2444776.2444791`. doi:`10.1145/2444776.2444791`.
10. Fischer, K., Karsch, S.. Modelling security relevant context an approach towards adaptive security in volatile mobile web environments. In: *International Conference on Web Science, Koblenz, Germany*. 2011, .
11. Johnson, G., Agrawala, A., Billionniere, E.. A framework for shrink-wrapping security services. In: *Proceedings of the 2010 IEEE International Conference on Services Computing*; SCC '10. Washington, DC, USA: IEEE Computer Society. ISBN 978-0-7695-4126-6; 2010, p. 639–640. URL: `http://dx.doi.org/10.1109/SCC.2010.79`. doi:`10.1109/SCC.2010.79`.
12. Gupta, A., Miettinen, M., Asokan, N., Nagy, M.. Intuitive security policy configuration in mobile devices using context profiling. In: *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. 2012, p. 471–480. doi:`10.1109/SocialCom-PASSAT.2012.60`.
13. Dyer, J.S., Fishburn, P.C., Steuer, R.E., Wallenius, J., Zionts, S.. Multiple criteria decision making, multiattribute utility theory: The next ten years. *Management Science* 1992;**38 Issue: 5**:645–654. doi:`10.1287/mnsc.38.5.645ManagementScienceMay1992vol.38no.5645-654`.
14. Rosenbloom, E.. A probabilistic interpretation of the final rankings in {AHP}. *European Journal of Operational Research* 1997;**96**(2):371 – 378. URL: `http://www.sciencedirect.com/science/article/pii/S0377221796000495`. doi:`http://dx.doi.org/10.1016/S0377-2217(96)00049-5`.
15. Saaty, T.L.. *Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World*. Pittsburgh, Pennsylvania: RWS Publications; 1999. ISBN 0-9620317-8-X.
16. Cocea, M., Magoulas, G.. Context-dependent personalised feedback prioritisation in exploratory learning for mathematical generalisation. In: Houben, G.J., McCalla, G., Pianesi, F., Zancanaro, M., editors. *User Modeling, Adaptation, and Personalization*; vol. 5535 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg; Springer Berlin Heidelberg, p. 271–282. URL: `http://dx.doi.org/10.1007/978-3-642-02247-0_26`. doi:`10.1007/978-3-642-02247-0_26`.
17. Koumoto, Y., Nonaka, H., Yanagida, T.. A proposal of context-aware service composition method based on analytic hierarchy process. In: Nakamatsu, K., Phillips-Wren, G., Jain, L., Howlett, R., editors. *New Advances in Intelligent Decision Technologies*; vol. 199 of *Studies in Computational Intelligence*. Springer Berlin Heidelberg. ISBN 978-3-642-00908-2; 2009, p. 65–71. URL: `http://dx.doi.org/10.1007/978-3-642-00909-9_7`. doi:`10.1007/978-3-642-00909-9_7`.
18. Chen, D.N., Hu, P.J.H., Kuo, Y.R., Liang, T.P.. A web-based personalized recommendation system for mobile phone selection: Design, implementation, and evaluation. *Expert Systems with Applications* 2010;**37**(12):8201 – 8210. URL: `http://www.sciencedirect.com/science/article/pii/S095741741000477X`. doi:`http://dx.doi.org/10.1016/j.eswa.2010.05.066`.