A Context-aware Adaptive Security Framework for Mobile Applications*

Yaser Mowafi, Dhiah Abou-Tair, Tareq Aqarbeh
School of Information Technology and Engineering
German Jordanian University
Amman, Jordan
{yaser.mowafi; dhiah.aboutair; tareq.alaqarbeh}@gju.edu.jo

Marat Abilov, Viktor Dmitriyev, Jorge Marx Gomez
Carl von Ossietzky University
Department of Computing Science
26111 Oldenburg, Germany
{marat.abilov; viktor.dmitriyev; Jorge.marx.gomez}@uni-oldenburg.de

ABSTRACT
Mobile devices currently offer many value-added applications and services such as messaging, navigation, social networking, finance, and entertainment. As these mobile applications have access to users' personal information and are capable of gathering and transmitting trust sensitive information, posing security and privacy risks. In this paper, we propose a context-aware adaptive security framework for eliciting users' context information and adapting this information with mobile applications' network access control mechanism. The framework enforces the execution of mobile applications inside security incubators to control the communication between mobile applications and mobile device resources. Applications' access requests are analyzed based on user's context information collected from the mobile device sensors and the application security configuration.

Keywords
Mobile computing, context awareness, context-aware security, AHP, decision analysis.

1. INTRODUCTION

Significant advancements in mobile technologies have shifted personal computing to pervasive and ubiquitous computing. Today smartphones are equipped with various built-in sensors that are capable of collecting and providing high precision and accurate data, such as location, motion, acceleration, and rotation. Smartphone devices use these collected data to recognize and interpret users' surrounding environment. Mobile applications can then use this information to adapt their user interfaces accordingly. For example, a mobile smartphone 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 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' personal information either directly through user solicitation, or indirectly through explicit or implicit users' interactions with these applications. This unrestricted access poses 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. For example, consider the following scenarios:

- A user who shares her location data with a location-based service provider app to find the nearest gas station or any other point of interest, but faces the risk of revealing her current activity that is inferable from the same data.
- A user who is willing to share his location and accelerometer data with a fitness mobile app to provide health advisory, but faces the risk of revealing his personal daily activities that are also inferable from the exact data.

That said, ensuring users' security needs to start from the mobile devices. For example, [2] propose leveraging the level of privileges of mobile devices' owners in terms of trust and security controls, commonly set by default at low levels throughout the installation lifecycle of applications on these devices, to protect users' information from malicious attacks and/or intrusions. In addition, [3] propose a framework to shadow users' personal data in place that users wants to keep private to block network transmissions that contain such data. Similarly, [4] propose a just-in-time notifications that appear when users' personal data is subject to sharing and displays a visual summary of the shared subject data. However, such security control measures and much of the existing security management mechanisms are generally static, and do not take into account the dynamic nature of users' surroundings in mobility.

In order to address the security challenges of mobile devices, we propose a context-aware adaptive security framework for eliciting context information and adapting this information with security control measures. The framework consists of multi-security incubators, in each of which, a mobile application can be executed. The incubator 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 run the security and communication mechanism within the incubator. When a running mobile application attempts to get a network access, it triggers a security checking request in the incubator. The request is analyzed based on

ICCASA 2014, October 15-16, Dubai, United Arab Emirates

DOI 10.4108/icst.iccasa.2014.257495

both the users' context information, collected from the mobile device sensors, and the application security settings using Analytic Hierarchy Process (AHP) method. In turn, the security control mechanism yields a secure or insecure network access alert prior to users' launching of the mobile application. We validate the proposed framework by implemented our security control mechanism in Android Operating System (OS) running on mobile devices.

The remainder of this paper is structured as follows. In Section 2, we describe the proposed context-aware adaptive security framework architecture. Section 3 presents a prototype and evaluation of our security mechanism for Android OS on mobile devices. Section 4 reviews related work. We conclude the paper with final comments.

2. FRAMEWORK ARCHITECTURE

In order to protect users' information and enhance security of mobile devices, a context-aware adaptive security framework has been developed. The framework uses context information and dynamically adapts the security settings of mobile applications for different situations and user actions. Context entails a variety of aspects –such as location, time, network, etc. – that are dynamically combined together to create a certain context. Context aspects are utilized to adapt the security level required by each mobile application.

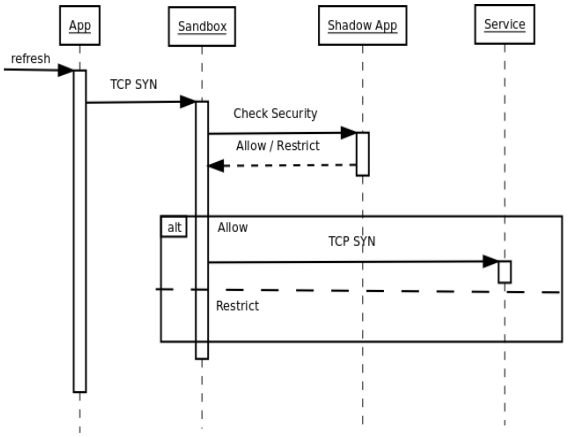


Figure 1. The UML Sequence Diagram of the frame work security mechanism

The proposed security framework consists of a mobile application incubator, or sandbox, and a context shadow application. The sandbox is built inside the mobile OS. Mobile application data, code execution, and network access are all concealed within the sandbox. Hence, a network access request can only go through the sandbox. To avoid any changes to mobile OS, the security component is implemented as a shadow application.

Fig. 1 illustrates the UML Sequence Diagram of the framework security mechanism. When a mobile application attempts to get a network access, the application sends TCP SYN request as part of a TCP handshake. This triggers a security checking method in the sandbox which is forwarded to the shadow application. The shadow application analyzes the request considering the security level and responds back to the sandbox with a secure or insecure network access. The security level is defined based on both the users' context information, collected from the mobile device sensors, and the users' security settings. The security settings provides users with a mechanism to prioritize their security level of each context aspect relative to the other context aspects. Fig. 2 presents the UML Component Diagram of the context shadow application. The application consists of following components:

- Application component, which is the main component that manages all requests from the sandbox and provides security decision.
- AHP Factor Processor component, which processes the importance factors of context aspects using AHP method, which will be discussed below.
- Context component, which gathers and categorizes the context information.

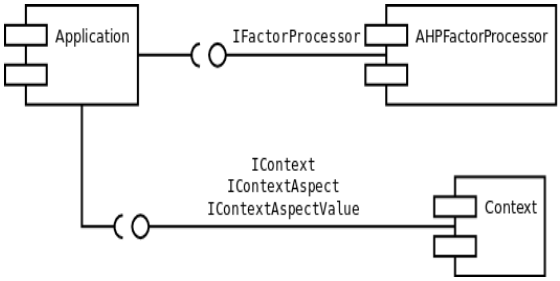


Figure 2. Shadow application component diagram

Fig. 3 shows the processing of security service requests in the shadow application. As shown in the Figure, when the shadow application receives an access request from the sandbox, it activates the Controller object. The Controller object loads the application security configuration and initializes a 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 security configuration to make the appropriate security decision. This decision will then be returned to the sandbox.

Given that context aspects are dynamically combined together, where each context aspect contributes a certain portion to the overall context. Hence, from a decision making perspective it will be necessary to consolidate these contexts into single integrated decision problem. Such consolidation allows for establishing a multi-criteria decision making (MCDM) [5]. A popular methodology for dealing with MCDM problems is Analytic Hierarchy Process (AHP) method [6]. AHP has been widely used in a variety of policy selection and decision making [7], adaptive learning [8], and recommendation and feedback systems [9]. One of the advantages of the AHP method is its breakdown of unstructured complex decision problems into smaller constituent components in order to construct an integrative hierarchy of the components weights. Another advantage is its capability of handling both tangible and intangible criteria that entails a systematic procedure in the thought process [10].

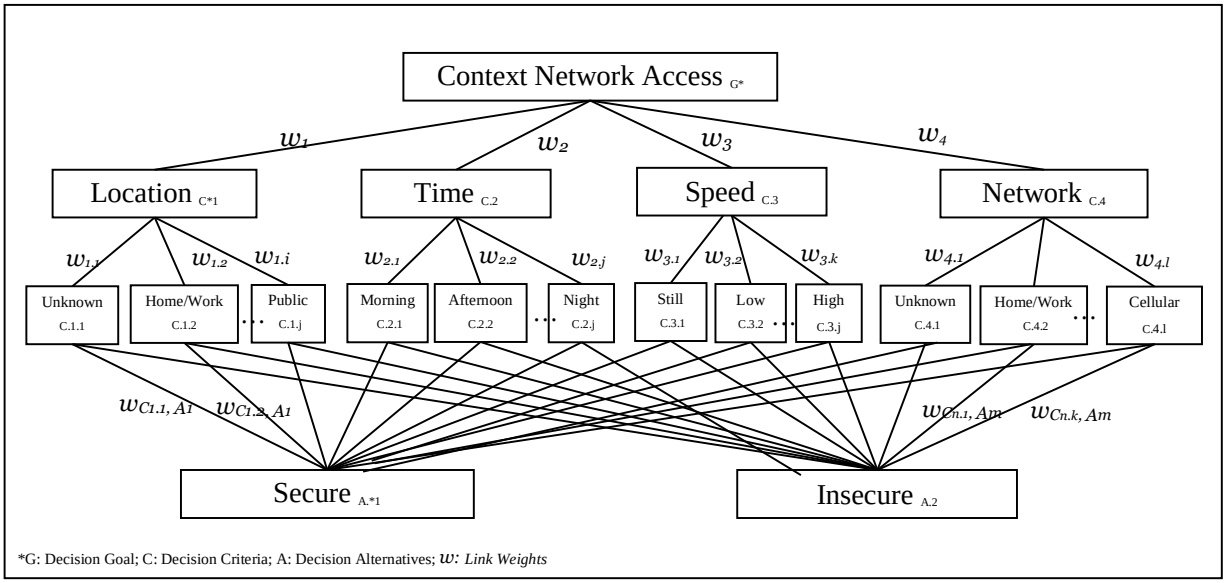


Figure 4. AHP hierarchy structure

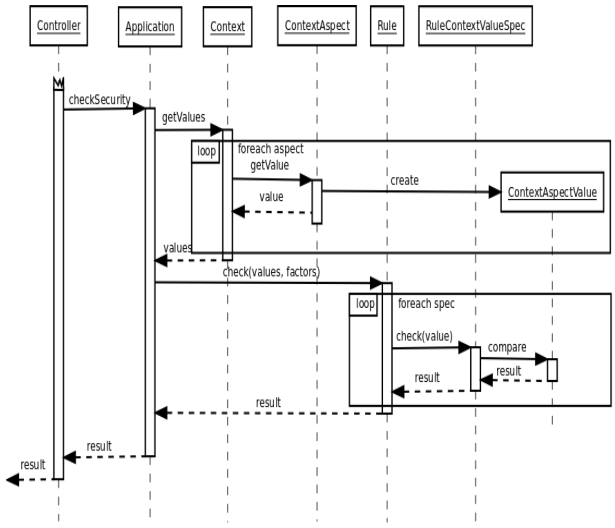


Figure 3. Processing of the request in the shadow application

When applied in decision problems, AHP assists in describing a general decision operation by decomposing the decision problem into a multi-level hierarchic structure. The top of the hierarchy represents the problem decision goal; the bottom denotes the decision problem alternatives A_1... A_i; and the decision criteria C_i and Sub-criteria $C_{i,j}$ are in the middle level. Connecting the criteria and the decision goal at the one hand, and the decision criteria with the alternatives at the other hand represent the AHP decision tree. The link weights ω_i and ω_{ij} are determined through a pair-wise comparison of C_i *and* $C_{i,j}$, respectively.

We apply the AHP method to perform a paired comparison among the context aspects (i.e., network, location, time, and speed) to determine the relative weights of the mobile application network access decision alternatives (Secure network access, Insecure network access), as shown in Fig. 4.

The AHP decision making process involves the following steps [10]:

- Developing a hierarchical structure that represents the key elements of the decision problem. The top of the hierarchy represents the overall objective, or the decision goal, and the bottom represents the decision alternatives. The middle level between the top and bottom represents the relevant criteria and sub-criteria of the decision problem.

- Assessing the influence of each alternative on the criteria and sub-criteria, by conducting pair-wise comparisons of the component elements for each alternative in the hierarchy.

- Utilizing the pair-wise comparisons, AHP applies an eigenvalue method to determine the weighted values for each component at each level of the hierarchy. For example, a pair-wise comparison of q elements' weights, ω_1, ω_2,… ω_q is performed via composing the following comparison matrix.

$$\begin{pmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \frac{w_1}{w_3} & \cdots & \frac{w_1}{w_q} \\ \frac{w_2}{w_1} & \frac{w_2}{w_2} & \frac{w_2}{w_3} & \cdots & \frac{w_2}{w_q} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \frac{w_q}{w_1} & \frac{w_q}{w_2} & \frac{w_q}{w_3} & \cdots & \frac{w_q}{w_q} \end{pmatrix}$$

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 $_j$th element with the $_i$ th element. This results in the comparison matrix being a reciprocal matrix satisfying $a_{ij} = 1/a_{ij}$. 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.

- Consolidating the weighted values, using component measure priorities assigned by the decision maker or analyst to create an overall top level decision value for each alternative.

3. PROTOTYPE IMPLEMENTATION AND EVALUATION

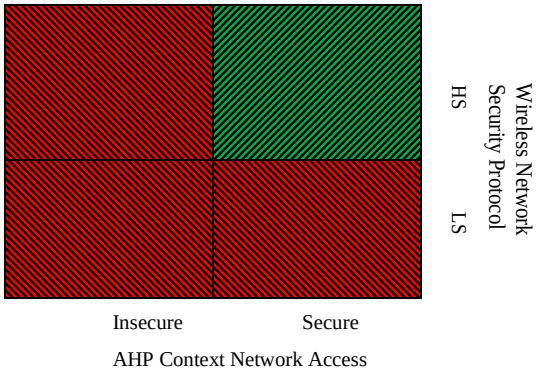
We developed a prototype application of the proposed security control mechanism in Android OS on mobile devices. The prototype architecture extends the programmable features built in Android OS through the definition and implementation of control components that aim to equip the mobile device with context-aware adaptive security features in run-time. The application enforces the execution of mobile applications inside a shadow application security incubator that controls the network access of these applications. As a use case, we select Facebook mobile application to implement and validate the security control mechanism lifecycle.

Table 1. Context aspects and states

Context Aspects	States			
Location	Unknown	Home	Work	Public
Time	Morning	Afternoon	Evening	Night
Speed	Still	Low	Medium	High
Network	Unknown	Home	Work	Cellular

For the sake of this work, we select four different context aspects, which can be retrieved in most current existing Android smart phones. Table I shows the selected context aspects along with their different states. For example, Network context aspect can have the following states: Unknown, Known network connection (i.e. Home or Work network), and Cellular network. Note that the application allows users to add and/or to modify the naming of the context aspects states.

We extend the AHP context security check algorithm (Fig. 3) to incorporate the evaluation of the wireless network security protocol of mobile applications network access request. The algorithm uses the instantaneous measures of both criteria to estimate the network access security risk level as one of low (GREEN) or high (RED). To do this we use two thresholds (Fig. 5). The first threshold corresponds to the calculated AHP context security level with respect to the context aspects relative weights (location, network type, time, and speed) and the relative weights of their corresponding current states. The second threshold tallies the wireless network security protocol that is detected upon the mobile application network access request. A Wi-Fi Protected Access (WPA) indicates a low security (LS) network protocol, while a Wi-Fi Protected Access 2 (WPA2) indicates a high security (HS) network protocol. WPA2 provides most secure communication among protected access protocols via the implementation of intricate encryption techniques [11].



HS: High security (WPA2) protocol
LS: Low security (WPA) protocol

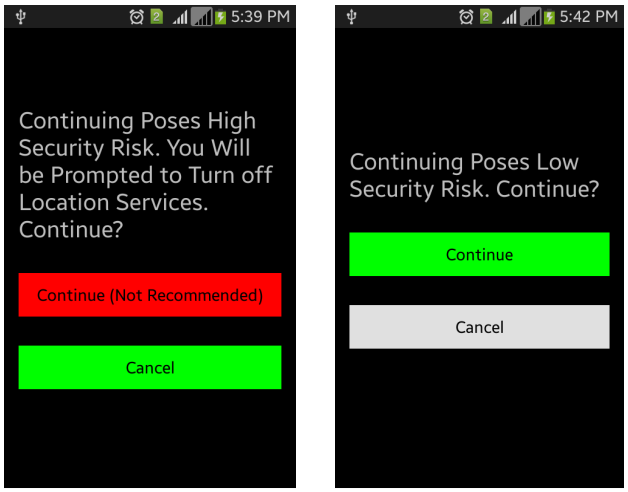
Figure 5. Security network access mapping

For example, Fig. 6 (a) 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 security 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. It also prompts the user to turn the location services off prior to launching the Facebook application, had the user decided to do so.

Alternatively, Fig. 6 (b) contemplates 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 security level yields a relative weight above the fiftieth percentile threshold. A detected WPA2 wireless network security protocol, or HS, in turn yields a low security risk level (GREEN). Hence, prompting the user to continue with launching the Facebook application.

In order to examine our security framework performance, 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 eight undergraduate university students affiliated participants (5 males and 3 females). Participants' age ranged from 19 to 23 years old with a mean age of 21. The participants are frequent mobile devices users, own Android mobile devices, and considered themselves as frequent users of mobile applications. Participants were offered an extra bonus points towards their course grade for their participation in the study.



(a) High security risk (b) Low security risk

Figure 6. Screenshots of the shadow application network access

After installing the security framework shadow application on their mobile devices, participants were briefed about the shadow application functionality and the security setting options. Participants were then instructed to run our logging 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 388 observations of launching attempts of Facebook via the shadow application security framework, with an average of seven different network access loggings per user per day. The collected data were divided into 90% of training data, and the remaining 10% for testing. The results showed a classification accuracy of 93% with an average Euclidian distance of 0.006. Euclidian distance ranges from 0 for the perfect classifier and square root of two for incorrect classification.

4. RELATED WORK AND MOTIVATION

The wide spread use of mobile devices and their integration with personal computing in different domains have shifted the paradigm of how security needs to be handled. For example, [12] proposed a so-called TaintDroid to provide real-time analysis of more than 20 mobile applications access to users' private information. The authors found considerable instances of potential misuse of such applications towards users' private information. Similarly, [13] investigate how permissions and privacy could play a role in users application selection decisions. The study found that presenting privacy information in a clearer fashion, could assist users in choosing applications that request fewer permissions.

Various research initiatives have explored the use of security relevant context with focus on delegation of access control rights based on environmental contexts. For example, [14] deployed logic-programming that incorporates context information to encode different types of access control security operations. Similarly, [15] utilize context-aware information in programming personalized role permission for granting access for services and information resources. In addition, [16] propose an ontology-based frame work that utilizes context information to derive security access control measures of mobile devices assets, such as messages, based on the confidentiality level of these assets. Other efforts also focused on semantic technologies for context representation to form access control mechanisms for mobile web services [17, 18]. However, the aforementioned approaches are exclusively constrained to provide users' access control based on context information and individual role.

Others [19], propose a context-aware usage control model, which takes into account context information, such as the spatial and time data to enforce ongoing policy defined by user during runtime to data access (i.e., data and files) and resource usage (i.e., CPU utilization and battery power). However, the framework relies heavily on users to define their policy on data and resources in a context-aware and fine- grained manner to perform evaluation based on the user definition rules. Our proposed framework aims to provide dynamic per- application context-aware adaptive security control measures at run-time.

Other research focuses on context-aware authentication and authorization policies for augmenting network security in ubiquitous computing environments [20]. For example, [21] explored context-aware scalable authentication (CASA) as a way of balancing security and usability for authentication by enabling easy access in commonplace everyday situations, such as home; while requiring more secure authentication in less common unidentified places. In addition, [22] proposed a context profiling framework using location WiFi and Bluetooth to infer appropriate access and sharing policies for sensitive data on the mobile device. Finally, [23] proposed CRePE, a context-related user policy enforcement framework for smart phones. CRePE allows the user to define a preset of security policy rules that depend on the location context, such as enabling Bluetooth service only when the users' location is at home or work, but not when traveling or being at train. In our proposed framework, the network type is included along with other context aspects to continuously perform security control measures. In addition, our framework provides a generalized infrastructure that can be configured for many different applications.

Finally, [24] propose a context-aware usage control model ConUCON, which takes into account context information, such as the spatial and time data to enforce ongoing policy defined by user during runtime to data access (i.e., data and files) and resource usage (i.e., CPU utilization and battery power). However, the framework relies heavily on users to define their policy on data and resources in a context-aware and fine-grained manner to perform evaluation based on the user definitions.

5. CONCLUSIONS

In this paper, we proposed a context-aware adaptive security framework that incorporates users' context, collected from mobile device sensors, with security enforcement policy decisions. The framework applies analytic hierarchy process (AHP) structured technique for dynamically evaluating users context, and provides the appropriate

security control decision. As a proof of concept, we used the Facebook mobile application as a use case to assess the impact of our proposed security management mechanism. Preliminary evaluation results have revealed the efficacy of our framework in providing security management control features based on real-time assessment of users' surrounding context.

6. REFERNCES

[1] P. Persson and Y. Jung, "Nokia sensor: from research to product," in *Proceedings of the 2005 conference on Designing for User eXperience*, ser. DUX '05. New York, NY, USA: AIGA: American Institute of Graphic Arts, 2005. http://dl.acm.org/citation.cfm?id=1138235.1138297

[2] A. Distefano, A. Grillo, A. Lentini, and G. F. Italiano, "Securemydroid: Enforcing security in the mobile devices lifecycle," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW '10. New York, NY, USA: ACM, 2010, pp. 27:1–27:4. http://doi.acm.org/10.1145/1852666.1852696

[3] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: Retrofitting android to protect data from imperious applications," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: ACM, 2011, pp. 639–652. http://doi.acm.org/10.1145/2046707.2046780

[4] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, ""little brothers watching you": Raising awareness of data leaks on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, USA: ACM, 2013, pp. 12:1–12:11. http://doi.acm.org/10.1145/2501604.2501616

[5] J. S. Dyer, P. C. Fishburn, R. E. Steuer, J. Wallenius, and S. Zionts, "Multiple criteria decision making, multiattribute utility theory: The next ten years," *Management Science*, vol. 38 Issue: 5, pp. 645–654, 1992.

[6] Rosenbloom, "A probabilistic interpretation of the final rankings in {AHP}," *European Journal of Operational Research*, vol. 96, no. 2, pp. 371 – 378, 1997. http://www.sciencedirect.com/science/article/pii/S037722179600049 5

[7] Y. Koumoto, H. Nonaka, and T. Yanagida, "A proposal of context-aware service composition method based on analytic hierarchy process," in *New Advances in Intelligent Decision Technologies*, ser. Studies in Computational Intelligence, K. Nakamatsu, G. Phillips-Wren, L. Jain, and R. Howlett, Eds. Springer Berlin Heidelberg, 2009, vol. 199, pp. 65–71. http://dx.doi.org/10.1007/978-3-642-00909- 97.

[8] M. Cocea and G. Magoulas, "Context-dependent personalised feedback prioritisation in exploratory learning for mathematical generalisation," in *User Modeling, Adaptation, and Personalization*, ser. Lecture Notes in Computer Science, G.-J. Houben, G. McCalla F. Pianesi, and M. Zancanaro, Eds. Springer Berlin Heidelberg, Springer Berlin Heidelberg, vol. 5535, pp. 271–282. http://dx.doi.org/10.1007/978-3-642-02247-0 26

[9] D.-N. Chen, P. J.-H. Hu, Y.-R. Kuo, and T.-P. Liang, "A web-based personalized recommendation system for mobile phone selection: Design, implementation, and evaluation," *Expert Systems with Applications*, vol. 37, no. 12, pp. 8201– 8210, 2010. http://www.sciencedirect.com/science/article/pii/S095741741000477X

[10] T. L. Saaty, *Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World*. Pittsburgh, Pennsylvania: RWS Publications, 1999.

[11] National Institute of Standards and Technology NIST 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[12] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung,P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, ser. OSDI'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6. http://dl.acm.org/citation.cfm?id=1924943.1924971

[13] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: ACM, 2013, pp. 3393–3402.

[14] G. Johnson, A. Agrawala, and E. Billionniere, "A framework for shrink-wrapping security services," in *Proceedings of the 2010 IEEE International Conference on Services Computing*, ser. SCC '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 639–640. http://dx.doi.org/10.1109/SCC.2010.79

[15] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," in *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '08. New York, NY, USA: ACM, 2008, pp. 113–122. http://doi.acm.org/10.1145/1377836.1377854

[16] K. Fischer and S. Karsch, "Modelling security relevant context an ap- proach towards adaptive security in volatile mobile web environments," in *International Conference on Web Science, Koblenz, Germany*, 2011.

[17] H. Shen and Y. Cheng, "A context-aware semantic-based access control model for mobile web services," in *Advanced Research on Computer Science and Information Engineering*, ser. Communications in Computer and Information Science, G. Shen and X. Huang, Eds. Springer Berlin Heidelberg, 2011, vol. 153, pp. 132–139. http://dx.doi.org/10.1007/978-3-642-21411-0 21

[18] R. L. Anand Dersingh and A. Jost, "Context-aware access control using semantic policies," in *Ubiquitous Computing And Communication Journal (UBICC) Special Issue on Autonomic Computing Systems and Applications*, 2008, vol. 3, pp. 19–32.

[19] G. Bai, L. Gu, T. Feng, Y. Guo, and X. Chen, "Context-aware usage control for android," in *Security and Privacy in Communication Networks*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, S. Jajodia and J. Zhou, Eds. Springer Berlin Heidelberg, 2010, vol. 50, pp. 326–343. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-16161-2 19

[20] A. Mihovska and N. Prasad, *Adaptive Security Architecture based on EC-MQV Algorithm in Personal Network (PN)*, 2007, pp. 433–437.

[21] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, “Casa: context-aware scalable authentication,” in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS ’13. New York, NY, USA: ACM, 2013, pp. 3:1–3:10. http://doi.acm.org/10.1145/2501604.2501607

[22] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, “Intuitive security policy configuration in mobile devices using context profiling,” in *Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust*, ser. SOCIALCOM-PASSAT ’12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 471–480. [Online]. http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.60

[23] M. Conti, V. Nguyen, and B. Crispo, “Crepe: Context-related policy enforcement for android,” in *Information Security*, ser. Lecture Notes in Computer Science, M. Burmester, G. Tsudik, S. Magliveras, and I. Ili, Eds. Springer Berlin Heidelberg, 2011, vol. 6531, pp. 331–345. http://dx.doi.org/10.1007/978-3-642-18178-8 29

[24] Jajodia, S., J. Zhou, et al. (2010). Context-Aware Usage Control for Android. Security and Privacy in Communication Networks, Springer Berlin Heidelberg. **50:** 326-343.

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