Continuous Context-Aware Device Comfort Evaluation Method

Jingjing Guo, Christian Damsgaard Jensen, Jianfeng Ma

Continuous Context-Aware Device Comfort Evaluation Method

Jingjing Guo[1], Christian Damsgaard Jensen[2], and Jianfeng Ma[1]

[1] School of Computer, Xidian University, Xi'an, 710071, China
[2] Department of Applied Mathematics & Computer Science, Technical University of Denmark, DK-2800 Kgs. Lyngby, Denmark

Abstract. Mobile devices have become more powerful and are increasingly integrated in the everyday life of people; from playing games, taking pictures and interacting with social media to replacing credit cards in payment solutions. The security of a mobile device is therefore increasingly linked to its context, such as its location, surroundings (e.g. objects and people in the immediate environment) and so on, because some actions may only be appropriate in some situations; this is not captured by traditional security models. In this paper, we examine the notion of *Device Comfort* and propose a way to calculate the sensitivity of a specific action to the context. We present two different methods for a mobile device to dynamically evaluate its security status when an action is requested, either by the user or by another device. The first method uses the predefined ideal context as a standard to assess the comfort level of a device in the current context. The second method is based on the familiarity of the device with doing the particular action in the current context. These two methods suit different situations of the device owner's ability to deal with system security. The assessment result can activate responding action of the device to protect its resource.
Keywords: context-aware, mobile device, device comfort.

1 Introduction

Mobile devices, such as smartphones, tablets and laptops are growing in both popularity and capability. A large amount of sensing capabilities has been embedded into these mobile devices [3], which enables them to establish their context, such as where a device is, what is it used for, etc. Although there are lots of methods [4] proposed to secure mobile devices, e.g. using technologies such as machine learning [1] or probabilistic approaches [12]), most of them consider the security status of a mobile device from the user's perspective, that is to say, they consider the owner-device relationship. The concept of *device comfort* proposed by Marsh et al. [6] draws a grand blueprint that a mobile device can be smart enough to perceive its current context and synthesize the cognized cues, then use the internal models to reason about its security status under the cognized context (including its user).

We use device comfort to measure the feeling of a mobile device in terms of the security status of an operation in the perceived context, such as "a user is checking the photos in the private album on a bus at 10 a.m." or "a medical professional is accessing the healthcare data in a pub using an unknown wireless network" [8]. If the device feels

uncomfortable about performing an action in a specific context, it can express its concerns, but the final decision to proceed is up to the user [7]. Storer et al. have examined user interface designs to express these concerns [11]. Because of the uncertainty of the environment, the result of security policy enforcement maybe wrong, while it is also not a wise option to make a decision without considering it. Morisset et al. presented a formal model for soft enforcement [9]. Soft enforcement means the agent in charge of enforcing a security policy can influence the agent in charge of making the decision rather than force the decision maker to adopt a certain action or leave them make a decision. The optimal influencing policy they proposed took both the control of the influencer and the environment uncertainty into account.

Marsh divides device comfort into three levels: basic comfort level, general comfort level and situational comfort level, with the accuracy of the considered context varying from low to high. The general comfort level is calculated based on the basic comfort level. Situational comfort level is calculated based on both of the two other comfort levels, which should consider the user, physical and virtual environment and the concrete behaviour of other entities. The literature on device comfort defines the general ideas of this concept, but there are few concrete examples of how to measure the comfort level of a mobile device and enforce suitable behaviour in the real world.

In this paper, we propose two methods for evaluating the situational comfort level of a mobile device. The aim of these methods is to reason about whether an action is suitable to be done in the current sensed context even if the action has passed the verification of the traditional access control method (identity ID and password and so on). We propose this computational method to assess the sensitivity of a specific action running on the mobile device in the current context and provide an approach to measure the difference between two contexts in an action's perspective. The first proposed method uses the predefined ideal context as a standard to assess the comfort level of a device in the current context. The second evaluation methods can monitor the status of the mobile device continuously rather than enforcing a static security policy used in traditional access control methods, which allows better reasoning about the risk of running an action in a certain context.

The rest of this paper is organized in the following way. Section 2 explores the notion of device comfort and describes how to represent contextual factors and their influence on the situational comfort level. We present the first method for calculating device comfort in Section 3. The second method (familiarity based method) is given in Section 4. Finally, we present conclusions and outline a few directions for future work in Section 5.

2 Mathematic Expression of Contextual Factors

As mentioned earlier, security of mobile applications has become increasingly dependent on the context [2],[10]. We define a specific context in which the device is currently involved as a tuple $C = \langle c_1, c_2, \cdots, c_n \rangle$, where each element (c_i) represents the value of a certain context factor, such as the device's physical location, the current time of day, the name of the network to which the device is connected, the surrounding devices, etc. Depending on the action, the different context factors that may influence the de-

vice's feeling about the security implications of performing that particular action may carry different weight. For example, the feeling of a mobile device about doing a type of action A(such as checking the mailbox) depends only on its physical location, so the current time and the network to which the device is connected are not important, but another type of action B(such as accessing a confidential file on the company's server) may depend on both its physical location and the network to which it is connected. We therefore say that different types of actions are sensitive to different context factors. We use another tuple $S^A = \langle s_1^A, s_2^A, \cdots, s_n^A \rangle$ to indicate the feature of an action A where s_i^A indicates the sensitivity of the device's comfort level about doing A to context factor c_i and we have $0 \leq s_i^A \leq 1 (1 \leq i \leq n)$, $\sum_{i=1}^{n} s_i^A = 1$. The intention behind this normalization is to measure the importance of each context factor using uniform criteria. If action A is more sensitive to context factor c_i than to c_j, s_i^A should be bigger than s_j^A. We define the sum of all elements is equal to 1 to meet the range of the computation result of the comfort level shown below.

3 Predefined-Standard Based Method for Situational Comfort Level Assessment

This method suits situations where the owner of a device wants to ensure that a certain type of action is only allowed in a specific predefined context. In this case, the ideal context should be defined and stored in the device beforehand as the standard to reason about the device's feeling. Taking the location as an example, like Marsh said in [5], there are some places where the device should be less comfortable in sharing its data with other devices than other places, so a device in a Comfort Zone can enhance its comfort, while in a Discomfort Zone, the comfort will be decreased. If the sensed context is different from the owner's assumption, the device will feel uncomfortable. The more difference there is between them, the lower the device's comfort level will be.
We assume that the predefined context for a certain type of action A given by device's owner is $P = \langle p_1, p_2, \cdots, p_n \rangle$. We then use the following equation to measure the difference between the perceived context $C = \langle c_1, c_2, \cdots, c_n \rangle$ and the predefined context $P = \langle p_1, p_2, \cdots, p_n \rangle$ when doing action A. We use a function D to compute the difference between two contexts to a certain action A and it is defined as: $D : C_1 \times C_2 \rightarrow D_{C_1 C_2}$, where $D_{C_1 C_2}$ is the variable to indicate the result of the function $D(C_1, C_2)$. Equation (1) is the function to compute the difference between context C and P to action A.

$$D_{CP} = D(C, P) = \overline{\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} - \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}} \cdot \begin{pmatrix} s_1^A \\ s_2^A \\ \vdots \\ s_n^A \end{pmatrix} \tag{1}$$

The "$-$" in Eq.(1) is the operator used to measure the difference between two values of the same context factor. Its meaning depends on the concrete meaning of each context factor. For example, if the factor is physical location, "$-$" could be a method to compute the distance between two locations; if the factor is the network to which the device is

connected, "$-$"will become a compare operator to judge whether the two networks are the same; and so on. It is obvious that the difference between each c_i and p_i ($i \in [1, n]$) should be normalized, so that the metric of each $c_i - p_i$ which is used to compute D_{CP} is the same. The operator"$\overline{x}$"in Eq.(1) is the function which maps $c_i - p_i$ to a certain difference level which is a real number between 0 and 1 (0 means exactly the same and 1 is exactly the opposite), so we know $D_{CP} \in [0, 1]$. As with the "$-$" operator, the mapping rule of "$\overline{x}$"in terms of each context factor depends on the concrete meaning of the factor and the device owner's preference.

If context C matches with context P, D_{CP} will be zero. The more difference between them, the bigger D_{CP} will be, and consequently the device will feel more uncomfortable. Here the meaning of "match" is not completely equal to the word "same". For example, if the value of an element in C (c_i) is different from the value of the corresponding element in P (p_i), while s_i^A is zero, then this difference won't impact the comfort level of the device in terms of action A, because action A is not sensitive to the ith context factor. In this case, we also say context C matches with context P, even if they are not, strictly speaking, the same.

We use $1 - D_{CP}$ to measure the comfort level of a device about doing an action in a certain context. We define a comfort threshold T_c and a discomfort threshold T_{dc} to map $1 - D_{CP}$ to three comfort levels. If $1 - D_{CP} \geq T_c$, the device feels the security status is safe and it feels comfortable; if $T_{dc} \leq 1 - D_{CP} < T_c$, the device feels the security status is fair and its comfort level falls between comfortable and uncomfortable; if $1 - D_{CP} < T_{dc}$, the device senses it may be compromised and feels uncomfortable.

4 Familiarity Based Situational Comfort Level Evaluation Method

Sometimes, the owner of the device cannot give a clear concept of a desirable context for an action. In this case, the device will consider the familiarity of doing the action in a certain context to measure its comfort level. If an action has already been done in a context many times without problems, the device will feel more familiar with the context for that action. The more familiar the device is with the current context of doing the action, the more comfortable the device feels, and vice versa. We use Eq. (1) to measure the difference between two contexts. Because of the limited precision of most sensed information (such as GPS coordinates), we consider two contexts the same if the difference between them is sufficiently small. In order to verify whether two contexts encountered by action A can be seen as the same, we define an equivalence relationship "$\sim$" for two contexts, so that all the contexts of A which have equivalence relationship "$\sim$" can be seen as the same and should be classified to one equivalence class. More contexts within an equivalence class means that the device will feel more comfortable to do the action in the context which belongs to the equivalence class.

The definition of "$\sim$" is: Assume P and P' are two contexts within the context set of action A , which means that action A has been done in both contexts P and P'. We say $P \sim P'$, if $D_{PP'} \leq \sigma$, where σ is the boundary condition used to distinguish two contexts defined by the owner.

When the device senses a new context C_{new}, when A is being performed, it must determine which equivalence class of A to use. If the new context is close enough to an

existing equivalence class, C_{new} should be added to that class. When an equivalence class already has many contexts in it, how do we then measure the distance between the new context and the equivalence class? We can learn from the physics method of computing the distance from one point to an object in the space. In physics, a point is computed to represent the center of the object and the distance between the tested point and the center point can be seen as the distance between the tested point and the object. Here we also define a core for an equivalence class to represent the feature of the contexts within this equivalence class. Assume an equivalence class of A is $X = \{C^1, C^2, \cdots, C^n\}$, ($C^i$ is the contexts belonging to X), the core of it is $X_{core} = avg(X) = \{c'_1, c'_2, \cdots, c'_n\}$, c'_i is the average value of the ith context factor in all the contexts (C^i) within class X, while how to compute the average value depends on the concrete meaning of the factor. If C_{new} and the core of an available equivalence class have the equivalence relationship, this means C_{new} is close enough to the contexts within this class and C_{new} should be added to it. If there is no available equivalence class whose core has equivalence relationship with C_{new}, a new equivalence class should be established where C_{new} is both the only context in it and the core of it. If there is a new member adding to an available equivalence class, the core of this class must be updated accordingly.

Adding a new context to an existing equivalence class requires the identification of the equivalence class of A that closest to C_{new}. One situation that may happen is that C_{new} is equally close to more than one existing equivalence classes of A, so we should decide to which class C_{new} should be added. Because the differences between C_{new} and each of these classes are the same, we should use other metrics to decide C_{new}'s destination. In this paper, we adopt the class which has the maximum cardinal number among all the candidate equivalence classes. For example, if the new context C_{new} shows that the device may be either in the owner's home or in the neighbour's home, this could happen when the owner is using it in his or her garden, we add C_{new} to the owner's home because the owner rarely uses the device in his or her neighbour's home compared to using this device in his or her own home, i.e. probability that the device's owner is in his or her own home is greater than at the neighbours. Finally, we use the ratio of the cardinal number of the selected class to the maximum scale of the action's equivalence class A as the device's comfort level. When the device obtains the value of $comfort\_level$, then it can map it into the corresponding comfort status using the same method mentioned in predefined-standard based method.

The strategy of adopting the maximum scale class as the new context's final destination may not suit all cases, so other metrics can also be adopted, such as take the minimum scale class or just select a class among the candidate classes randomly. If we use the maximum strategy, the scale of the selected class will become larger and larger, while if the minimum strategy is adopted, the scale of these candidate classes will finally tend to the same, moreover, the random strategy cannot explicitly influence the scale evolution of those candidate classes. It is obvious that these different scale evolution situations will lead to different result of the *comfort_level*, so different mapping rules should be used to map the different values of *comfort_level* to a certain comfort level of the device. Here, we used the ratio of the scale of the current context's equivalence class to the maximum scale of the action's equivalence class as the result of the *comfort_level*,

while in different scenario or with different preference of the mapping rule, other methods can also be adopted to get the desired result.
In the following, we present the algorithm for measuring the comfort level of a device to do an action A in a new perceived context C_{new}. We assume there are m existing equivalence classes of action A noted $\{X^1, X^2, \cdots, X^m\}$ and use $[C]_\sim$ to represent the equivalence class to which context C belongs. $\sigma$is the boundary to determine whether two contexts have the equivalence relationship mentioned above.

Algorithm 1 familiarity based comfort level evaluation method

Require: new perceived context "C_{new}",σ,all existing context equivalence class $\{X^i, i \in [1, m]\}$ of action A stored in the device
Ensure: the comfort level of doing A in context C_{new}
  for each equivalence class X^i **do**
    $m = \min\{D_{X^i_{core}C_{new}}, i \in [1, m]\}$; // $D_{X^i_{core}C_{new}}$ is the difference between X^i_{core} //andC_{new} calculated by Eq. 1
  end for
  if $m > \sigma$ **then**
    create a new equivalence class X^{m+1};
    put C_{new} into X^{m+1};
    $X^{m+1}_{core} = C_{new}$;
  else
    create an empty set E;
    for each X^i **do**
      if $D_{X^i_{core}C_{new}} == m$ **then**
        put X^i into E;
      end if
    end for
    put C_{new} into class X^f ($|X^f| = \max\{|X^i|, X^i \in E\}$);
    update X^f_{core};
  end if
  $comfort\_level = \frac{|[C_{new}]_\sim|}{\max\{|X^i|\}}$;

5 Discussion and Future Works

In this paper, we presented two methods for evaluating the feeling of a mobile device in terms of security when an action is requested in a certain context. The different evaluation results can activate corresponding measures to protect the resource on the device. Although a thorough discussion of implementation issues and technical solutions goes beyond the scope of this introductory work, some of the issues are worth being mentioned and briefly discussed.
With respect to the sensitivity of a kind of action A, we use a tuple (tuple S^A mentioned in Section 2))to represent its sensitivity to different contextual factors. From Eq. (1) we can see that applying different sensitivity tuples to an action, we will obtain different

comfort levels for performing this action given the same context. So properly assigning the weigh of each contextual factor is crucial to get a satisfactory evaluation result. There are already some consensuses on the sensitivity of some actions, e.g. we should check our bank account in a privacy space rather than a public place, and so on. There are,however, also situations where the situational factors are more complex, so more works need to be done in the future on how to properly assign the weight of each factor. Similar to the assignment of weights to the situational factors, it is possible to use different metrics for measuring the distance between two, or more, contexts. We currently propose to use the distance between the center of a context equivalence class and a perceived context as the distance between the equivalence class and the perceived context, rather than compute the shortest distance between the perceived context and any context within the equivalence class. We can consider the context space of a mobile device as an $N-$ dimension space, each contextual factor is an axis, so a concrete context is a point in this space and an equivalence class is a mass within this space. The more contexts within an equivalence class gathers at a point, the greater the density of this point will be. So we should measure the center of the equivalence class just as find the center of gravity of a non-uniform density distribution object in physics. If we select any context within the class to compute the distance, the range of the context within the equivalence class will be expanded indefinitely, because a point (perceived context) may be close to the edge of an object (the equivalence class) but far away from its center of gravity (the center of the equivalence class). In this case, the context equivalence class will lost the meaning of equivalence and it can not represent a type of context anymore. Because the assignment of the sensitivity vector will influence the distance between two given contexts, different values assigned to the situational vector will lead to different evolution of a context equivalence class given the same perceived contexts sequence. It is possible that all the contexts can be included into the same equivalence class, and it is also possible that each perceived context falls into different equivalence class. To get a desired evaluation result, the relationship between the assignment of the situational vector and the evolution of the context equivalence class of an action should be further studied.

A drawback of the familiarity based method is that the accuracy of the evaluation result depends on the scale of the obtained context data. A device needs a lot of context data to obtain the usage pattern of each action. So the evaluation result will be more accuracy with the increasing use of the device. If we want to get a satisfactory effect, maybe some tests should be done before the first formal use of the method in a mobile device to get enough usage data.

Now we are exploring a security policy language to represent our methods, so that we can further implement them in the future. We will continue to improve the methods to better evaluate the security relevant feeling of the mobile devices in a certain context to enhance its security. Concretely speaking, we will study the method which is able to self-adjustment according to its performance feedback from the user, so how to get these feedbacks from user will also be considered in our future work.

Acknowledgements

This work was partly supported by the China Scholarship Council,the Program for Changjiang Scholars and Innovative Research Team in University (China) under Grant No.IRT1078, the Key Program of NSFC-Guangdong Union Foundation (China) under Grant No.U1135002 and the Major National S&T Program (China) under Grant No.2011ZX03005-002.

References

1. Bose, A., Shin, K.G.: Proactive security for mobile messaging networks. In: Proceedings of the 5th ACM Workshop on Wireless Security. pp. 95–104. WiSe '06, ACM, New York, NY, USA (2006), http://doi.acm.org/10.1145/1161289.1161307
2. Chen, G., Kotz, D., et al.: A survey of context-aware mobile computing research. Tech. rep., Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College (2000)
3. Khan, W., Xiang, Y., Aalsalem, M., Arshad, Q.: Mobile phone sensing systems: A survey. Communications Surveys Tutorials, IEEE 15(1), 402–427 (First 2013)
4. La Polla, M., Martinelli, F., Sgandurra, D.: A survey on security for mobile devices. Communications Surveys Tutorials, IEEE 15(1), 446–471 (First 2013)
5. Marsh, S.: Comfort zones: Location dependent trust and regret management for mobile devices. Proceedings LocationTrust (2010)
6. Marsh, S., Briggs, P., El-Khatib, K., Esfandiari, B., Stewart, J.A.: Defining and investigating device comfort. Journal of Information Processing 19, 231–252 (2011)
7. Marsh, S., Noël, S., Storer, T., Wang, Y., Briggs, P., Robart, L., Stewart, J., Esfandiari, B., El-Khatib, K., Bicakci, M.V., et al.: Non-standards for trust: Foreground trust and second thoughts for mobile security. In: Security and Trust Management, pp. 28–39. Springer (2012)
8. Marsh, S., Wang, Y., Noël, S., Robart, L., Stewart, J.: Device comfort for mobile health information accessibility. In: Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. pp. 377–380. IEEE (2013)
9. Morisset, C., Yevseyeva, I., Groß, T., van Moorsel, A.: A formal model for soft enforcement: Influencing the decision-maker. In: Security and Trust Management, pp. 113–128. Springer (2014)
10. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: A survey. Communications Surveys & Tutorials, IEEE 16(1), 414–454 (2014)
11. Storer, T., Marsh, S., Noël, S., Esfandiari, B., El-Khatib, K., Briggs, P., Renaud, K., Bicakci, M.V.: Encouraging second thoughts: Obstructive user interfaces for raising security awareness. In: Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. pp. 366–368. IEEE (2013)
12. Xie, L., Zhang, X., Seifert, J.P., Zhu, S.: pbmds: a behavior-based malware detection system for cellphone devices. In: Proceedings of the third ACM conference on Wireless network security. pp. 37–48. ACM (2010)