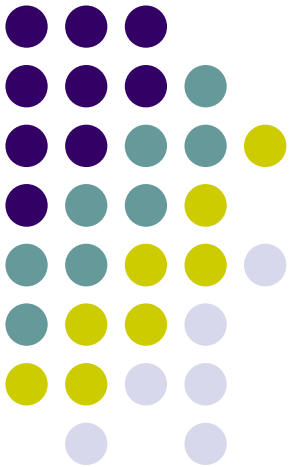
Ubiquitous and Mobile Computing CS 528: *The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior*

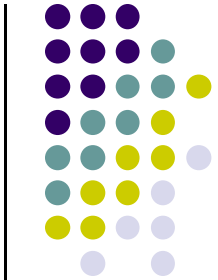
Chu Xu

Computer Science Dept.

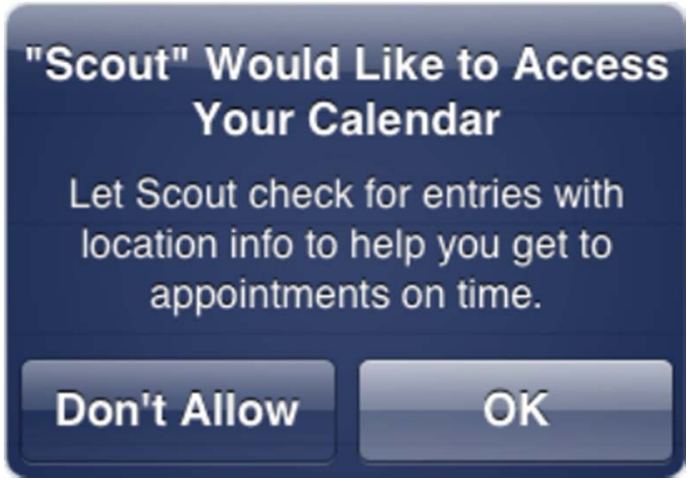
Worcester Polytechnic Institute (WPI)



Introduction/Motivation

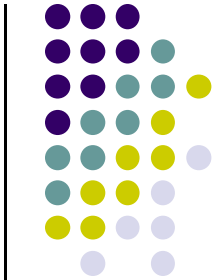


- Permission request dialog on iOS.
- Optional explanation, purpose string.



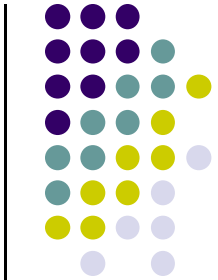
- Allow or don’t allow, that is the question.

Introduction/Motivation



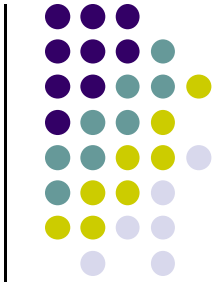
- User Behavior
  - 700 smartphone users
- How many apps with permission request dialog had purpose strings
  - 4000 apps
- Why developers would like to add purpose string or not
  - 30 developers

Related Work



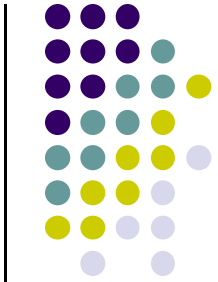
- Threats
  - Malicious app
  - Unintentional access to personal data
- How to present request
  - iOS, WP: Runtime warning
    - Habituated to warnings
  - Android: Install-time warning
    - Few users read

Methodology: User Behavior



- Task 1:
  - Screenshot of request with explanation
- Task 2:
  - Screenshot of request without explanation
- Task 3:
  - Request of a fake app, Party Planner, with purpose string of a pool of 14

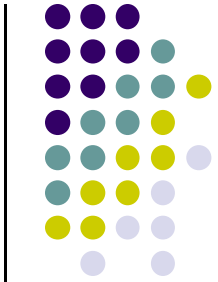
Methodology: User Behavior



Purpose String	Approval Rate
Control: "Contact access is required for this app to work properly."	52.5% of 59
"Let Party Planner use your contacts to autocomplete email addresses."	70.2% of 47
"To find friends, we'll need to upload your contacts to Party Planner. Don't worry, we're not storing them."	69.5% of 59
"Party Planner would like to access your address book to show you the cheapest attractions by your contacts' location. We won't use your contact information for any other purposes."	66.7% of 48
"Your contacts will be used to find your friends."	65.5% of 58
"In order to find your friends, we need to send address book information to Party Planner's servers."	62.5% of 48
"Have more fun with your friends on Party Planner."	58.7% of 46
"Easily search for and share event information with the people who matter most to you."	57.5% of 40
"Your contacts will be uploaded to our secure server. This data is maintained securely and is not shared with another party."	52.9% of 34
"Your contacts will be used to find your friends. They won't leave your phone."	51.5% of 33
"In order to find your friends, we need to send address book information to Party Planner's servers using a secure connection."	51.0% of 51
"Your contacts will be transmitted to our servers and used to find your friends."	46.2% of 39
"Party Planner would like to access your address book to show you the cheapest attractions by your contacts' location."	45.5% of 55
"Party Planner would like to access your address book to show you the cheapest attractions by your contacts' location and other purposes."	38.8% of 49
Total:	56.8% of 666

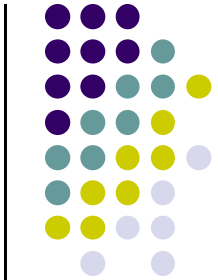
Table 4. Pool of app purpose strings for the fictitious Party Planner app, as well as their associated approval rates. The first purpose string was used as a control condition because it conveys no information about why the app is requesting access.

Methodology: User Behavior



- Question 1:
  - Name of app? Previously used?
- Question 2:
  - Open-ended questions
    - What information would be accessed if “OK”?
- Question 3:
  - Rate the purpose strings of Party Planner from “strongly agree” to “strongly disagree”

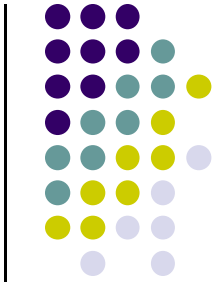
Methodology: User Behavior



1. *It helps me make a more effective decision about the sharing of my information.*
2. *It is useful.*
3. *It gives me more control over the sharing of my information.*
4. *It makes it easier to decide on the sharing of my information.*
5. *It allows me to quickly decide on whether to share my information.*
6. *It allows me to efficiently decide on whether to share my information.*
7. *It addresses my concerns over the sharing of my information.*
8. *I am satisfied with it.*
9. *It makes me more comfortable deciding on whether to share my information.*
10. *It is clear and easy to understand.*
11. *The language used is simple and natural.*
12. *I feel like it is necessary for me to make an effective decision about the sharing of my information.*

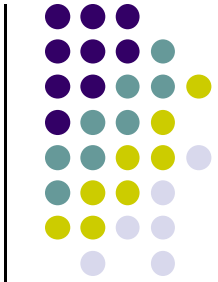
Table 2. Each participant answered 12 questions on a 7-point Likert scale ("strongly agree" to "strongly disagree"). We took the average of these 12 responses to create a "satisfaction score."

Result: User Behavior



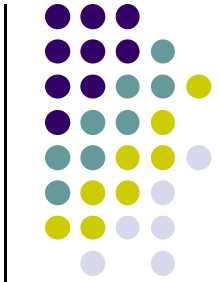
- Purpose and Control
  - 568 participant approved 74% of request with purpose string and 66% of request without
  - Statistically significant by Wilcoxon Signed Rank
- People are more likely to allow request with a purpose string.

Result: User Behavior



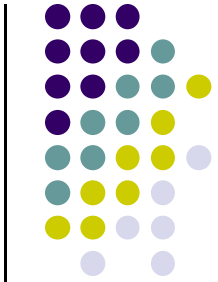
- Choice of Text
  - Scores varied but no significant approval rate
- People are more likely to allow request with a purpose string but usually they don’t care or understand the content of the strings.

Methodology: Adoption

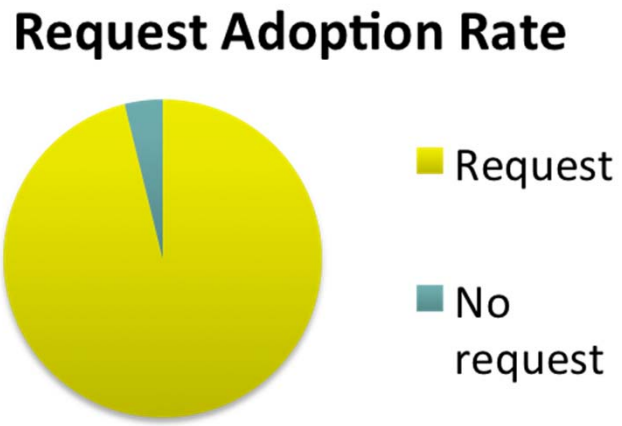


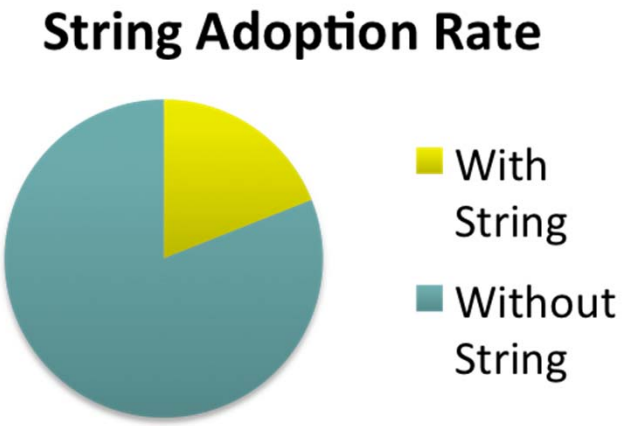
- 4,400 free apps from App Store
- Number of apps with purpose string
  - From app's plaintext metadata file
- Number of apps with request
  - By static analysis on decrypted binaries
- Manual Testing
  - Manually find those numbers of 140 app to prove the accuracy

Result: Adoption

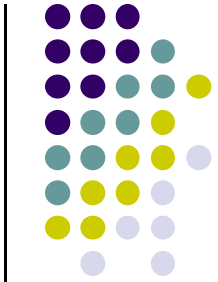


- Adoption rate
  - 80% of apps request access
  - Only 19% of them have purpose strings
  - Manual adoption rate is 17.5%



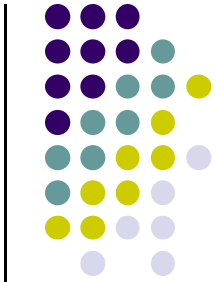


Methodology: Developer Opinions



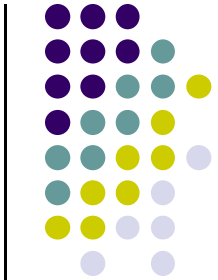
- 30 iOS developers and two popular apps
  - Description of Vine and Scout
  - Whether the apps need permission request
  - If yes, write a purpose string for it

Result: Developer Opinions



- Developer Awareness
  - 28 think permission request necessary, 17 claimed to be aware of purpose string, 7 did use purpose string
  - No relationship with years of developing experience
- Developer Attitudes
  - User benefit works
- Developers use few purpose strings due to lack of awareness and this is because Apple's poor documentation of this feature

Conclusion



- Apple need to improve the document of purpose string to let developers be aware and use it
- Developers can used purpose strings to let users know why
- User need to read and make a trade-off between privacy and functionality

References

- Agarwal, Y., and Hall, M. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, MobiSys '13, ACM (New York, NY, USA, 2013), 97–110.
- Amer, T. S., and Maris, J. B. Signal words and signal icons in application control and information technology exception messages – hazard matching and habituation effects. Tech. Rep. Working Paper Series–06-05, Northern Arizona University, Flagstaff, AZ, October 2006. **http://www.cba.nau.edu/Faculty/ Intellectual/workingpapers/pdf/Amer JIS.pdf**.
- Apple Inc. What's New in iOS. **https: //developer.apple.com/library/ios/releasenotes/ General/WhatsNewIniOS/Articles/iOS6.html**, January 28 2013. Accessed: September 15, 2013.
- Benisch, M., Kelley, P. G., Sadeh, N., and Cranor, L. F. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Comput. 15*, 7 (Oct. 2011), 679–694.
- Bravo-Lillo, C., Komanduri, S., Cranor, L. F., Reeder, R. W., Sleeper, M., Downs, J., and Schechter, S. Your attention please: designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM (2013), 6.
- Brustoloni, J., and Villamar´ın-Salomo´n, R. Improving Security Decisions with Polymorphic and Audited Dialogs. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, ACM (2007), 76–85.
- *Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. Location disclosure to social CHI 2014, One of a CHInd, Toronto, ON, Canada relations: why, when, & what people want to share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '05, ACM (New York, NY, USA, 2005), 81–90.*
- *Yang, J. Smartphones in use surpass 1 billion, will double by 2015. http://www.bloomberg.com/news/ 2012- 10- 17/smartphones- in- use- surpass- 1- billion-will-double-by-2015.html, 2012.*
- *Xia, H., and Brustoloni, J. C. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In Proceedings of the 14th International Conference on the World Wide Web, WWW '05, ACM (New York, NY, USA, 2005), 489–498.*

References

- *Egelman, S., Cranor, L. F., and Hong, J. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems, CHI '08, ACM (New York, NY, USA, 2008), 1065–1074.*
- *Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. 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, OSDI '10, USENIX Association (Berkeley, CA, USA, 2010), 1–6.*
- *Enck, W., Octeau, D., McDaniel, P., and Chaudhuri, S. A study of Android application security. In Proceedings of the 20th USENIX Security Symposium, SEC '11, USENIX Association (Berkeley, CA, USA, 2011), 21–21.*
- *Felt, A. P., Greenwood, K., and Wagner, D. The effectiveness of application permissions. In Proceedings of the 2nd USENIX Conference on Web Application Development, WebApps '11, USENIX Association (Berkeley, CA, USA, 2011), 7–7.*
- *Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, ACM (New York, NY, USA, 2012), 3:1–3:14.*
- *Fisher, D., Dorner, L., and Wagner, D. Short paper: Location privacy: User behavior in the field. In Proceedings of the Second ACM workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '12, ACM (New York, NY, USA, 2012), 51–56.*
- *Kelley, P. G., Benisch, M., Cranor, L. F., and Sadeh, N. When are users comfortable sharing locations with advertisers? In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11, ACM (New York, NY, USA, 2011), 2449–2452.*
- *Kim, S., and Wogalter, M. Habituation, dishabituation, and recovery effects in visual warnings. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 53, SAGE Publications (2009), 1612–1616.*
- *Langer, E., Blank, A., and Chanowitz, B. The Mindlessness of Ostensibly Thoughtful Action: The Role of "Placebic" Information in Interpersonal*

References

- *Lever, C., Antonakakis, M., Reaves, B., Traynor, P., and Lee, W. The Core of the Matter: Analyzing malicious*
- *traffic in cellular carriers. In Proceedings of the ISOC Network & Distributed Systems Security Symposium, NDSS '13 (2013).*
- *Lin, J., Amini, S., Hong, J., Sadeh, N., Lindqvist, J., and Zhang, J. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the Second ACM workshop on Security and Privacy in Smartphones and Mobile Devices, UbiComp '12, ACM (New York, NY, USA, 2012), 51–56.*
- *Mongolo. Rasticrac v3.0.1.*
- *http://iphonecake.com/bbs/viewthread.php?tid= 106330&extra=page%3D1, April 17 2013. Accessed: September 15, 2013.*
- *Nissenbaum, H. Privacy as contextual integrity. Washington Law Review 79 (February 2004), 119.*
- *Pearce, P., Felt, A. P., Nunez, G., and Wagner, D. AdDroid: privilege separation for applications and advertisers in Android. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS '12, ACM (New York, NY, USA, 2012), 71–72.*
- *Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. Understanding and capturing people's privacy policies in a mobile social networking application. Personal Ubiquitous Comput. 13, 6 (Aug. 2009), 401–412.*
- *Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. Crying wolf: an empirical study of SSL warning effectiveness. In Proceedings of the 18th USENIX Security Symposium, SEC '09, USENIX Association (Berkeley, CA, USA, 2009), 399–416.*
- *Thompson, C., Johnson, M., Egelman, S., Wagner, D., and King, J. When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources. In Proceedings of the Ninth Symposium on Usable Privacy and Security, ACM (2013), 1.*