

Projekt TDP028:

Tekniskt PM

1 Introduktion

Nu för tiden är det stort fokus på säkerhet och integritet på nätet. För appar är en stor del av detta *permissions*, appen frågar användaren om den får tillgång till känsliga delar av operativsystemets resurser och information. Eftersom min app kommer vilja ha tillgång till exempelvis användarens nuvarande plats, är det bra att ha en inblick i hur användare ser på *permissions*.

Hur, och när, ska man fråga användaren om *permissions* för att inte skrämma bort den?

2 Intryck vid installation

Google ändrade 2015 hela *permission*-systemet i och med Android 6.0 Marshmallow från att fråga användaren om den godkänner alla *permissions* vid installation till att fråga användaren första gången appen försöker använda en känslig del av systemet [1], har det blivit tydligare för användaren vilka *permissions* som appen vill att användaren accepterar.

Det har visats att om appen frågar om alla *permissions* vid installation är det ytterst få som läser dom, och ännu färre som förstår dem [1] [2]. Detta innebär att jag kommer behöva tänka över vilka *permissions* som är nödvändiga.

3 Intryck i appen

Det har visats att användare gärna vill veta vad appen gör i bakgrunden, och i cirka 50 procent av fallen kunna blockera de *permission*-baserade anrop som appen gör i bakgrunden [1].

Samtidigt vill användare bli störda i onödan av pop-up fönster som frågar om tillåtelser hela tiden. Ifall jag som utvecklare kör på en säker infallsvinkel vid utveckling av appen och frågar om fler *permissions* än nödvändigt, kommer det att utsätta användaren för onödiga *permission*-förfrågningar, samt öka effekten av buggar och sårbarheter i appen [3].

4 Utvecklingsstrategier för appen

För att inte utsätta användaren för sårbarheter i appen, och för att användaren ska få en övergriplig förståelse för vad appen faktiskt gör, får jag noga fundera ut vilka *permissions* som faktiskt behövs för att appen ska fungera.

Google reviderar hela tiden *permissions* vilket gör att de som behövs för en äldre version av Android kan ha *permissions* som är onödiga i den aktuella versionen [3]; detta kan påverka vilken api-nivå jag som utvecklare bör inrikta mig mot. Onödiga *permissions* kan även få användaren att avinstallera appen, om de anser att de är utanför deras ”comfort zone” [2].

Referenser

- [1] A. B. A. H. S. E. D. W. K. B. Primal Wijesekera, ”Android Permissions Remystified: A Field Study on Contextual Integrity,” i *24th USENIX Security Symposium (USENIX Security 15)*, Washington, D.C., USINEX Association, 2015, pp. 499-514.
- [2] E. H. S. E. A. H. E. C. D. W. Adrienne Porter Felt, ”Android Permissions: User Attention, Comprehension, and Behavior,” *Proceedings of the Eighth Symposium on Usable Privacy and Security*, vol. III, nr 1, pp. 1-14, 2012.
- [3] E. C. S. H. D. S. D. W. Adrienne Porter Felt, ”Android permissions demystified,” *Proceedings of the 18th ACM conference on Computer and communications security*, vol. 1, nr 18, pp. 627-638, 2011.