CAB240 Information Security
Semester 2 2016
Mobile Security Investigation Part II

This task continues the investigation into the information security issues associated with your personal mobile device – smartphone or tablet - that you began in Part I. For each security issue (related to Operating system, Application and User behaviour) discussed in Part I, find resources that outline control measures that you could apply to prevent the issue or reduce the level of harm.

Recall the NSTISSI 4011 cube from Lecture 1. Control measures can involve technology, policy and practices, or education training and awareness. If you identified a similar issue several times in your Part I submission (say, confidentiality breaches for multiple reports), provide different means of dealing with this in your Part II submission, rather than providing the same control measure multiple times.

Your PART II submission will consist of:

1. An introduction giving a brief description of your information assets, an overview of your use of the device, and the issues you were concerned about in Part I (summarise Part I Sections 1 and 2 into 1 page or less)
2. A report on *control measures that could be applied to mitigate the information security issues associated with the mobile device operating system* you discussed in Part I Section 3.
3. A report on *control measures that could be applied to mitigate the information security issues associated with the mobile device application* you discussed in Part I Section 4.
4. A report on *control measures that could be applied to mitigate the information security issues associated with user behaviour* you discussed in Part I Section 5.
5. A conclusion relating the application of the control measures to the identified information security issues, and summarising the information security position for your personal mobile device.
6. Bibliography (include reference details for the resources related to control measures)

NOTE: Part II reports (Sections 2, 3 and 4) use a different template to Part I reports, this is given below:

Template

First submission article:

Title: Put the title of the article from your first submission here.

Author: Add the author's name here.

Reference details (if online article, give URL and date accessed): Add the reference details here.

Security goals compromised: Really brief summary from the first report here (correct it if you need to).

Threat/vulnerability/attack details: Again, very brief.

This submission: treating the risk

Suggested control measure and explanation:
Give an explanation of a control measure for the particular scenario. There may be a few different options, so pick the one you think is most effective - unless you have already used that option for a previous article. Is the control measure preventive, detective or corrective? How does it work?

Try to keep your explanation reasonably non-technical. Also, the control measure article need not be recently published. But it should be suitable for the scenario in the original article. If not, find a different article.

Limitations of this control measure:
To what degree does this protect the asset? Does it reduce the likelihood of an incident, or the consequence?
Does the control measure have any other impact (for example, on efficiency, battery power, user experience, require technical competence on the part of the device user, …)?