ENISA Smartphone Security Working Group
Expert Questionnaire

This questionnaire is the first step in ENISA's 2010 study on smartphone security risks. We will follow up the results by clarifying responses with individual experts and optionally with telephone conferences to discuss points of controversy. We will then use the group to review and contribute to a report based on the results. Our aim for 2010 is an overview of risks and best practice aimed at CIO/CSO level but also useful for political decision makers (e.g. deciding on research programmes).

We will follow this up with more detailed recommendations on specific risks identified. We would like to use this work to kick-start a dialogue between all the relevant stakeholders on smartphone security.

Please specify the platform(s) your answers apply to (e.g. Android, Apple, Blackberry, Ovi, Windows Phone 7) and **if they apply only to a particular target group** (e.g. business, government, consumers). We are looking for **specific vulnerabilities and threats, including examples of "in the wild" attacks** exploiting real-world vulnerabilities. **Please give references where possible**. We are not looking for long or polished answers – notes/bullets with pointers to more material are fine. Answers can be submitted in any format including email.

1. What are the top security risks affecting smartphones and in particular smartphone apps and marketplaces? You might want to consider the following areas in your answer or add ideas of your own:
   - Access control:
     - Cross-app access to processes
     - Cross-app access to data stores (including in back-end applications.)
     - Shared/covert communication channels between apps
   - Process authentication and key management
   - Application development, review and release processes (in-house and 3rd party), including vendor review of 3rd party apps.
   - What process exists to detect, mitigate, and patch vulnerabilities and exploits as they become widespread on smartphone devices?

- Anti-phishing measures (and prevention of identity theft).
- Resource usage (e.g. calls to premium numbers, battery, SMS).
- Vulnerabilities created by users bypassing phone security/access control policies (e.g. jailbreaking, rooting)
- Privacy and inference threats for sensor data and stored data
- Secure deletion of data
- Data integrity checks
- Data backup and retrieval, remote wiping and remote password resets in the case of loss or theft
- Data protection of removable media and remote backup locations.

2. What mechanisms exist to assure the authenticity of app developer/distributor identities? (technical, process, and legal)
3. What mechanisms are in place to assure the reliability of app reputation data?
4. What mechanisms are in place to prevent the misuse of sensor data, at the platform (OS) and the app level? How effective are these?
5. How serious in your opinion is the risk of surveillance through the analysis of combined sensor data sensors (e.g. accelerometer, camera, GPS)? What mechanisms are in place to prevent this?
6. How serious is the risk of coordinated and/or distributed attacks based on smartphones (e.g. smartphone based botnets, government/corporate data theft, sabotage, attacks on wireless networks etc...) – currently, and in the future?
7. What guidance is given on security best practices to app developers, through what channels?
8. What guidance is given on security best practices to end-users, through what channels?
9. What support channels does an *end user* have in case of security problems?
10. Do you envision capabilities that will allow alerting a smartphone user about a compromise of their device?
11. Please cite any relevant existing studies and papers on smartphone security.