Why has ENISA conducted this report on the topic of smartphone security?
80 million smartphones were sold worldwide in the third quarter of 2010, accounting for 20% of the total of mobile phones sold in this quarter. In the EU5 alone (UK, Germany, France, Spain, and Italy) the number of smartphone users increased to a total of 61 million. Smartphones are becoming increasingly important across the EU and therefore ENISA believes it is important to give an overview of the main information security risks and opportunities.

Who is the report for?
IT officers (CIO's, CSO's, CTO's et cetera) in business and public organisations to facilitate their evaluation and mitigation of the risks associated with adopting smartphones;

- Consumer safety bodies and consumers to enable them to minimise the risks of smartphone usage.
- European policymakers, to aid them in deciding on research policy and measures required to mitigate risks.

What does the report focus on?
The main focus of the report is to assess and rank the most important information security risks and opportunities for smartphone users and give prioritised recommendations on how to address them.

What approach have you used in your analysis to determine security risks?
We have consulted smartphone experts across vendors and IT organisations, as well as security officers in business and government organisations. They were asked to identify threats and to rate the likelihood and the impact of threats. This has been compiled into a list of the main risks.

What are possible assets that could be at risk in a smartphone?
Smartphones contain a lot of private data, and often also secrets such as banking credentials. In the case of employees, smartphones may contain corporate intellectual property and classified government information. Other assets at risks are personal data, reputation, but also money and confidential government or business documents.

What are the three main security risks associated with smartphone usage?
From an information security perspective smartphones have certain advantages over traditional PCs and mobile handsets:

- ○ **Data leakage resulting from device loss or theft**

Smartphones, being at the same time very valuable and pocket-sized, are more likely to be stolen or lost than other computing devices. If data on the device's memory or removable media is not sufficiently protected, an attacker can access it. The impact of such threats is high: Smartphones often contain credit card data, bank account numbers, passwords and account details, personal data, location history and addresses. Business phones, additionally, contain corporate sensitive emails and documents, client data, and business contacts.

○ **Unintentional disclosure of data**

Users are not always aware of all the functionality of applications. They may for example be unaware (or do not recall) that an app collects and publishes data about where they are located, *even if* users have given consent for this at install time or on first run. The website icanstalku.com (the smartphone version of pleaserobme.com) shows an example of this.

○ **Attacks on decommissioned smartphones**

Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives before decommissioning. But this is not yet happening with smartphones. At the same time, more and more smartphones are being recycled (market analysts say 100 million mobile phones per year by 2012). Smartphones contain large amounts of information, making them an increasingly attractive target for "smartphone dumpster divers".

What are the main information security opportunities for smartphone users?

From an information security perspective smartphones have certain advantages over traditional PCs and mobile handsets:

- **Sandboxing and capabilities**

Sandboxing is a security mechanism separating running applications. An application in a sandbox cannot access or manipulate data or functions of other applications for malicious purposes. Moreover smartphone operating systems are often based on a capability-based model. In this model, individual processes are granted separate privileges (called capabilities) which are by default limited, following the principle of least privilege. Both features limit the impact of malicious software.

- **Controlled software distribution**

An information security opportunity with respect to traditional PC's, is offered by the "walled garden" approach many smartphone vendors take to 3rd party software: by default, users can only add applications from a centrally controlled distribution channel. Only few users circumvent this restriction by unlocking their smartphone (for example, less than 10% of iPhone users unlock their smartphone). On most traditional PC's, by contrast, it is easy for users to install software from a variety of sources, which allows for so-called “drive-by download” attacks - a common way for attackers to infect PC’s.

- **Remote application removal**

Some smartphone vendors have built in functions that allow remote removal of applications from smartphones after installation (also known as a remote kill-switch). This feature, if used correctly by the smartphone vendor, mitigates the risks of malware.

What is an example of ENISA’s recommendations in the report?

The recommendations are expressed as a set of security policy controls which can be plugged into an IT department’s security policy. The recommendations are risk-based, addressing the risks one by one.

For example, for the consumer use case we recommend: End-users should configure the smartphone in such a way that it locks automatically after some minutes. Some smartphones allow visual passwords to ease the use of auto-lock features.

Recommendations for IT officers:

- For IT officers we recommend to have a policy rule on smartphone data confidentiality: Memory encryption should be used for the smartphone memory and removable media used in smartphones. It is recommended to check the security properties of encryption schemes or require certification.

Recommendations for smartphone industry:

- For example, to address the risk of unintentional disclosure, we recommend industry-wide privacy guidelines for app. Currently, every app deals with these issues differently. Standardization makes it easier for users to set the right settings. Also developers of smartphone apps and services should avoid unintentional data disclosure by choosing safe default settings (privacy and security by default).

The full report is available at:

For further details contact:

Marnix Dekker, Application security Officer, ENISA
marnix.dekker@enisa.europa.eu
Ulf Bergstrom, Spokesman for ENISA,
press@enisa.europa.eu Mobile: +30 6948 460143