

Priorities for future research on mobile privacy and security

Authors:

Ian Nordman (Nokia)

ian.nordman@nokia.com

Margareta Bjorksten (Nokia)

margareta.bjorksten@nokia.com

Date: 19 August 2002

1. BACKGROUND

Security issues have traditionally resulted in technology driven solutions on the mobile marketplace. This is in contradiction to privacy, which has emerged from a social and legislative environment not too familiar with the possibilities and constraints of technology. Over the past years privacy issues have not been sufficiently addressed on the Internet despite end users' growing privacy concerns. Many privacy aspects are often left out already in the design phase of new services. The primary reason is that privacy-enhancing technologies are only entering the market and are thus still not widely accepted.

The Mobile domain and the Internet domain will ultimately converge in the next generation of mobile networks. Many emerging business models will require effective flows of user data, which will virtually be insensitive to network borders. Governments, vendors, mobile operators and consumers must be proactive in order to identify and solve new privacy and security threats.

Public requirements on security and privacy-enabled technologies can result in many architectural approaches. Market fragmentation poses a real threat to an effective penetration of privacy and security technologies. Privacy and security are fundamental mobile commerce enablers and failure to develop open privacy standards could be detrimental to the long-term health of the whole industry.

2. AUGMENTED ELECTRONIC IDENTITIES

Use of standardized electronic identities is likely to become the common denominator for next generation mobile services. The idea is not new; today electronic identifiers are used globally: ID's describes customers and employees in companies' databases; governments use identifiers for identifying citizens and the mobile network transmits the caller-ID to the mobile handset just for mentioning some. However, novel uses of electronic identities need to explicitly make use of standardized privacy and security technologies in order to be widely adopted and gain end-user acceptance. In addition, as the sensitivity and amount of data related to electronic identities increase, the notion of end-users themselves appropriately controlling the usage of their electronic identities must become generally accepted. In other words, technologies should provide end users with

- The ability to securely attach personally identifiable and other information to their electronic identities
- The ability to securely manage the storage, use and distribution of data related to their electronic identities
- The ability to adjust levels of anonymity and pseudonymity

In the mobile domain, this augmented electronic identity brings up a framework, which essentially provides end users with the notion of Mobile Personalities.

Within the context of Mobile Personality, privacy means the state of making augmented electronic identities available to other entities without exposing these identities to privacy threats. These threats are unsolicited marketing (spamming), traceability, linkability (profile accumulation), discrimination, and loss of control over personal data and identity theft.

It is self-explanatory, that technologies within the mobile personality framework should be developed with the end-user view in mind. Such architectural systems would require well-defined and standardized mechanisms for managing the level of transparency vis-à-vis end-users.

The Mobile Personality framework should be considered as a viable and long-term approach when specifying end-user driven privacy and security instruments. However, standardization efforts need to be made in order to ensure interoperability across domains.

3. CONCLUSION

Privacy protection is proving to be one of the greatest challenges for the Internet and mobile environment. No one action can alone provide satisfactory privacy protection. Instead, a framework consisting of several supporting elements is needed to ensure sufficient security and working electronic privacy protection. The framework should include global directives, comprehensive national and sectoral laws, self-regulation, enforcement mechanisms, user education and privacy protection technologies.

In order to ensure progress in this field, developments of technical standards is needed that

- Maximize security and privacy sensitiveness in the management of electronic identities
- Direct critical points of decision over disclosure and usage of electronic identities and personal information to end-users
- Is designed with usability and end-user needs in mind.