Nikita Salnikov
O.M. Galushko, research supervisor
V.V. Gubkina, language adviser
SHEI “National Mining University”, Dnipropetrovsk

Some Problems with Securing Information on Mobile Connections

The issue of data leakage has always arisen from data at rest, data in transit, email, IM and various other internet channels, however now with the rise of mobile technology, data leakage is occurring with greater ease, whether by accident or malice. Accessing the Internet and specifically the World Wide Web from a mobile phone is common today. Almost every mobile phone today comes with an integrated web browser that can display HTML web pages and execute JavaScript. Almost all major web sites such as news sites, social networks, and shopping sites run websites that are optimized for small displays of mobile phones. Sophistications and deviousness of widely-prevalent PC-targeting viruses have been advancing over the years. And many different techniques that have emerged in that field are likely to be applied also to smart phones putting smart phones users at risk. For secure use, smart phones users, as in the case of PCs, should first be aware of what operating system is running on their phone model, and then implement required safeguard against viruses etc. while paying attention to security-related news.

To protect data three cryptographic algorithms are in common use nowadays: authentication, encryption and key management. For a long time, the level of defense was rather high, but eventually a number of vulnerabilities have been found. But it is strange, that no measures to eliminate these gaps in protection have been taken. Once there is a risk, the user needs to know how to understand that it is tapped.

The main abuse of this information leak is user tracking. In some countries one can do a reverse lookup of phone numbers. This means for those countries one can take a mobile phone number and actually determine the name (first and last) and user tracking is very likely since the phone number is internationally unique. Further the phone number will stay even if the user changes to a new mobile phone (e.g. after an upgrade or warranty replace). This enables reliable long term tracking possibilities. Large commercial and social networking sites that operate a mobile version of their site can collect this information to enrich the profile data that they already have about their users. As with everything, the numerous benefits of the ever increasing mobile age come with many challenges. There will always be numerous potential security risks brought about by the mobile and remote working age, however organizations all need to do what they can to curb or prevent these security breaches where possible. If corporations effectively combine the security measures available, encryption (in its many forms), DRM, DLP and CMS technologies, a virtually fool-proof data leakage prevention system can be accomplished. Corporations should make it a priority to meet the challenge of data leakage prevention or the beneficial remote productivity could end in corporate loss and not meet upcoming global compliance laws.