Evgeniy Goroshko
A.V. Gerasina, research supervisor
V.V. Gubkina, language advisor
SHEI “National Mining University”, Dnipropetrovsk

Emerging Trends of Information Security

The landscape of information security is going to be altered over the next several decades. There is the emerging trend nowadays which requires the computers to interact with each other directly in short-term relationships on behalf of, but not necessarily at the command of, humans. Here, the concerns about privacy and security become even greater. This emerging trend will have three major outcomes. One is to make the general public as a whole much more aware of and concerned about reliability issues in general, and security and privacy issues in particular.

The second outcome concerns the role the government will play with regards to these increased concerns. In general, the government will probably play a major role in increasing the security and robustness of the infrastructure since it is a national issue that goes beyond any single corporation. The third outcome is becoming the problem of security harder than ever.

We will not only need to protect, relatively long-term interactions between computers engaged in at the behest, of people (e.g, secure email), but short-term coalitions between computers acting essentially on their own. Due to the requirements of modern trends in the sphere of Information Technologies, the much research is focused on developing three main capabilities: the ability to quantify the value of information assets to determine the resources a penetrator is likely to expend to compromise various types of information; the ability to select a set of system properties to raise the cost of successfully compromising system security above the value of the assets protected by that system, and the ability to refine these properties into secure implementations.

The mentioned above capabilities for assessing the value of information and for protecting that information sufficiently still exist. These capabilities are tempered by financial environment to produce great pressure by using sophisticated security devices in systems whose functionality will be COTS supplied. Limited human resources may lead to remote system administration and, being coupled with frequently forming and dissolving coalitions will exacerbate an existing severe key management problem.

The increased presence and connectivity of computers in the future will lead to more severe security, dependability, safety, and timeliness requirements that must be balanced with one another. Finally, we must graduate beyond the fortress mentality that still permeates much computer security research and move to a penetration-tolerant paradigm with a supporting command and control architecture.