

## Security Systems and the War against Cyber Enemies

Name

College

Date

Perhaps, it would be quite poetic, theatrical and trivial, but modern development of security systems and various firewalls has a lot of similarities with arms military industry. The creation of every brand-new 'weapon', i.e. security software, implies the developing of flawless and absolute system which is capable to protect any IT program or server from outside threats. Just like national arms industry of one country, it competes with national arms industry of another. In IT industry, "another country-competitor" for security system developers is hackers and other cyber-criminals. There was, there is, and there will be a war between two sides of one big information system industry.

In fact, the creation of brand-new security systems inevitably provokes the designing of counter-measures. It is quite hard to develop a static security system, considering the dynamics of technological progress and advancement. According to specialists, it requires approximately two weeks on average for hackers to develop a 'cracking unit' for breaking any existent security system and firewall (Kizza, 2005). Every innovative decision pertaining to modification, improvement or enhancement of security system practically encounters with some innovative decision from cyber-attackers, who, in turn, pursue the goal to excel their opponents. The reality is so tough that contemporary software and security system developers have to modify their security products almost every month to provide quite stable and reliable protection. It is possible to mention the innovative security system of Ubisoft Company which included the keeping of information on the remote server divided on several fragments, what, initially, complicated the cracking in general (Rainie & Anderson, 2009). However, it took less than three weeks for hackers to crack the system and build automatically independent server located far from official server of Ubisoft. Therefore, the 'armament drive' will continue for a very long time.

## References

Kizza, J.M. (2005). *Computer network security*. Chattanooga, TN: Springer Science.

Rainie, H. & Anderson, J.Q. (2009). *The future of the Internet: Ubiquity, mobility, security*. Amherst, NY: Cambria Press.