Lecture X – Speaker John Doe

Three main messages from this lecture:

- IT crime is increasing rapidly and becoming more and more professional with viruses corresponding to products with their own business. The threads and infections are generated faster and in a global scale. This results into a “cat & mouse” game, where viruses are constantly designed and modified to retaliate against and respond to the new methods and mechanisms introduced to detect and protect against them. Catching the criminals becomes harder. At the same time, the generic public falsely assumes the situation is improving.

- Technically, malware today aims to attack the network elements for resources and processing in order to produce e.g. SPAM. As the security technology improves, new methods and vulnerabilities, such as the often not patched 3rd party products used in web browsers, to attack are also searched. Resulting distributes systems, such as botnets, are difficult to detect and protect against with viruses retaliating against security servers. So far, mobile phones have been pretty safe due to co-operation, however also here e.g. spyware is now emerging and available.

- The work in this company is arranged in three global shifts using automatic tools aside e.g. manual analysis. Technical edge is maintained through the customer sample base enabled by internet and with a tight co-operation towards the competitors.

My grade to the speaker: #

Personal comments. <Any additional comments or feedback to the lecturer>