Preventing unsolicited software

Anton Borg, BTH

I started as a Ph.D. Student this spring on a project financed by the .SE foundation. My research is summarized in the following paragraphs.

During the years we, as a society, have grown more and more dependent on email in our daily life. During these years we have seen a number of threats toward mail, such as unsolicited email (also known as spam) and forgery. This has led to the question of what threats exist against email and whether we have ways to mitigate these threats.

An increasing amount of unsolicited software are present in todays computer world, of which several fall under the category of spyware and adware, applications which operate in a legal grey zone. Some of these applications aid in the spreading of spam. In order to counteract this growing threat of unsolicited software, we today have several signature based detection and removal tools, similar to the antivirus software niche. These tools detect installed versions of the unsolicited software, meaning that it has already been operating for some time. But by then the damage might already be done and thus begs the question if there are alternative methods.

One way to prevent the spread of unsolicited software is to use a reputation system. By letting users rate applications it will be possible to discern those applications that are harmful to the end-user and allow the end-user to make an informed decision about whether to allow the application to be installed or to run. Can such a system be efficient and is it feasible? What aspects must one consider, e.g. how are different groups of users able to classify programs?

One reason why many anti-virus programs don't remove spyware and adware, is that the user have often agreed, through the end-user license agreement(EULA), to allow it's installation. Due to the way most EULA's are written, this goes unnoticed by the end-user. Research into using EULA analysis to identify spyware applications, has shown that this can be done by e.g. machine learning techniques. Using this information, would it be possible to use EULA analysis to provide additional information to users of previously mentioned reputation system and thus give the reputation of an application more weight?