A Large-Scale Study of the Time Required to Compromise a Computer System

Abstract:

A frequent assumption in the domain of cybersecurity is that cyberintrusions follow the properties of a Poisson process, i.e., that the number of intrusions is well modeled by a Poisson distribution and that the time between intrusions is exponentially distributed. This paper studies this property by analyzing all cyberintrusions that have been detected across more than 260,000 computer systems over a period of almost three years. The results show that the assumption of a Poisson process model might be unoptimal - the log-normal distribution is a significantly better fit in terms of modeling both the number of detected intrusions and the time between intrusions, and the Pareto distribution is a significantly better fit in terms of modeling the time to first intrusion. The paper also analyzes whether time to compromise (TTC) increase for each successful intrusion of a computer system. The results regarding this property suggest that time to compromise decrease along the number of intrusions of a system.