New Army models predict number of cyberattacks that pierce company networks

September 20 2017

Dr. Nandi O. Leslie was part of an Army Research Laboratory team that studied empirical data on actual successful cyber intrusions committed against a number of different organizations. These data were obtained from a provider of cyber defense services, which defended those organizations as clients. Credit: Jhi Scott, US Army Photographer

A new study from the U.S. Army Research Laboratory presents evidence that the number of cyber intrusions can be predicted, particularly when analysts are already observing activities on a company or government organization's computer network.

Researchers say new models that predict the number of intrusions would be of significant value to providers of cyber security and resilience services.

Dr. Nandi O. Leslie was part of the team that studied empirical data on actual successful cyber intrusions committed against a number of different organizations. These data were obtained from a provider of cyber defense services, which defended those organizations as clients.

The researchers were able to determine the correlation - or lack thereof—between the number of successful intrusions and observed features of an organization, for 41 organizations. The team looked at the security incident reports containing detailed information about malicious activities and computer security policy violations by users and operators; DNS traffic, collected with specialized and open source software for all organizations in this study; and other data sources describing a selected subset of features of each organization's network topology and cyber footprint. As a result, the researchers were able to propose four generalized linear models (GLMs) to predict the number of successful cyber intrusions into an organization's computer network, where the rate at which intrusions occur is a function of several observable characteristics of the organization.

Additionally, they analyzed regression results for adequacy of fit to the intrusions data. Among their key findings is that one of these models—the generalization of the Poisson regression model to the negative binomial GLM model—predicts the response variable appreciably better than others. They also demonstrate that the intrusions data exhibit sufficient regularity (in statistical sense), and the construction of a practically useful predictive model is feasible, said Leslie of ARL's Network Security Branch.

The key research question—which of the initially conjectured predictor variables should be included in the model—brought rather surprising findings, Leslie said.

"Several of the predictor variables that were recommended to the researchers by subject matter experts turned out to be lacking in influence or even misleading. For example, SMEs felt that the extent to which an organization is visible on the Internet, as measured for example by the number of records found related to that organization on the popular Google Scholar, would be a significant predictor of intrusion frequency. However, it turned out that such visibility alone is not a useful predictor of successful intrusions," Leslie said.

Yet another variable that the SMEs expected to be influential—the number of hosts within an organization's network—also turns out to be a less significant predictor for the NB GLMs than hypothesized by SMEs.

On the other hand, the researchers show that the number of violations of an organization's internal cyber security policies is a strong predictor of the number of intrusions.

"This finding is rather intuitive. Indeed, if users such as employees of the organization lack the discipline or knowledge to comply with organizational cyber hygiene policies, and if the organization is unable or unwilling to enforce its own policies, it is easy to expect that the organization's cyber defenses are poor, leading to more frequent intrusions. Less intuitive is the finding that the frequency of accesses by the organization's networks to the domains domestic.net and foreign.net are strong predictors of intrusions. Although it is not entirely clear why this should be the case, the researchers offer a possible explanation," Leslie said.

Importance of predictive model

Among client organizations, the numbers of intrusions differ dramatically by many orders of magnitude. Some organizations experience a large number of intrusions in a given time frame, whereas others may not experience any intrusions for a number of years. A specialized organization, such as a managed security service provider, is often used by an organization to provide cyber defense services. For a MSSP, the costs of doing business are heavily influenced by the number of intrusions experienced by its clients. Therefore, when a MSSP negotiates its fees with a new prospective client, it needs a model to estimate how many intrusions should be expected over some fixed time period.

Another example where such a model would be of high value is its use for actuarial purposes. In a broader sense, a model of this nature contributes to our fundamental understanding of cyber situational awareness and ways to monitor, quantify, and manage cyber risk. Finally, a model of this nature may offer clues toward enhancing the security posture and perhaps the design and operation of an organization's computing systems and networks. If the model indicates that certain characteristics are associated with an increased number of intrusions, the organization might be able to find ways to modify those characteristics.

This research is presented in a paper "Statistical models for the number of successful cyber intrusions", by Nandi O. Leslie, Richard E. Harang, Lawrence P. Knachel and Alexander Kott; the paper is to appear in a special issue of the *Journal of Defense Modeling and Simulation* in 2018.

More information: Nandi O Leslie et al. Statistical models for the number of successful cyber intrusions, *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* (2017). DOI: 10.1177/1548512917715342

Provided by U.S. Army Research Laboratory

Citation: New Army models predict number of cyberattacks that pierce company networks (2017, September 20) retrieved 26 April 2024 from https://phys.org/news/2017-09-army-cyberattacks-pierce-company-networks.html