Letters to the Editor

Measuring Security Risk of Networks Using Attack Graphs: A Critique

The article, titled above, (Noel, Jajadia, Wang, & Singhal, 2010) attempts to define a practical approach to evaluating systems security risks using the Monte Carlo simulation technique. Given the ongoing challenges of practically assessing investment in information security projects, a simple and usable metric, as defined by the authors, would constitute a very valuable tool for organizational decision support. Despite inherent limitations with the Monte Carlo method, which is well documented to be highly dependent on the quality of model inputs, the method presented by Noel et al would be useful in systems development at the design stages of project analysis.

Summary

From the security point of view, the challenge of modern information system design is the multitude and sophistication level of cyber-attackers, who constitute real threats to the ever-growing networks of organizations competing in the global economy. In ”Measuring Security Risk of Networks Using Attack Graphs,” Noel et al (July 2010) point out that system security analysis has matured beyond simply counting vulnerabilities, towards a necessity for understanding the interactions of those vulnerabilities. Such logical combinations naturally lend themselves to analysis using the Monte Carlo simulation technique, which takes into account non-linear logical relationships and individual probability distributions of input variables. Given the trade-offs between security risks, budget constraints, and availability of services (system updates, etc), maximum likelihood models resulting from Monte Carlo analysis provide a logical cost-benefit framework to evaluate the options an organization faces. To lay the groundwork for maximum likelihood analysis, the article highlights the probabilities arithmetic involved with conjunctive and disjunctive dependencies (in the context of attack paths logic); and offers Symantec DeepSight Threat Management System as a reference guide for model inputs, i.e. reported vulnerabilities likelihood and costs. A well-defined graphical framework of the model is presented, along with a fairly detailed, if simplified, case study analysis as an illustration. In particular, once information system data flow is specified and attack paths (graphs) are outlined, probabilities of different steps will need to be estimated in order to run the iterative simulation process of Monte Carlo analysis. In turn, this will generate a Compromise Likelihood probability for all decision options, enabling a cost-benefit analysis and a return-on-investment model –practical tools to enable fact-based decision processes. According to the article, total cost of an outcome is defined as a combination of expected loss (cost of recovery and likelihood of attack), and estimated cost of prevention measures. In addition to outlining a practical approach to evaluating costs of potential network changes based on attack-graph metrics, the authors provide a thorough sensitivity analysis methodology for assessing model specification (”input variable importance”) and robustness, with likelihood breakpoint criteria.

Usability

The challenge of organizational risk management is defined in part by the non-monetary value of return on investment in information technology projects. The aim of fact-based executive decision-making is to link systems development with an organizational business model and evaluate investment options based on well-defined cost-benefit analyses (Remenyi, Bannister, & Money, 2007). The article presents a simple and robust framework to address this challenge. The discussed methodology is based on well-established risk management practices, is rather easily implementable with currently available computing power, and allows the flexibility to accommodate a scalable set of parameters (Girao, Postolache, & Pereira, 2009). The discussion fits within the third generation of security research, which calls for cost-benefit analysis of security investments under the intrusion tolerance framework (Verissimo, Neves, & Correia, 2003).

The attack graphs methodology is firmly linked with industry research and is presented with a model evaluation framework in order to ease implementation. In the context of the System Development Life Cycle, well-specified Information Flow diagrams will be analyzed for security vulnerabilities during the design stages of system development (Whitman, 2009). Noel et al provide methodology to deepen the analysis of those vulnerabilities and link to cost-benefit analysis, which is a welcome notion in any practical setting.

Limitations

The Monte Carlo simulation method is a popular statistical technique, often used in modeling complex financial instruments -i.e. derivatives: options, swaps. The method is named after well-known casinos for its use in analyzing games of chance. It allows for bypassing complicated mathematical relationships in order to estimate likelihoods of outcomes based solely on the probability distributions of inputs, which are not limited to normality. Thus, the method is extremely flexible in terms of assumptions and easily scalable to accommodate a large number of variables. Monte Carlo simulations involve independent draws that increase the precision of results with an increase in the number of iterations (though at a slower rate). Because of the heavy dependence on specification of the model inputs, in this case system vulnerabilities (probabilities of attack and associated costs), iterative simulation results are only as good as the quality of these estimates. The authors offer two solutions: historical observations of the frequency of system attacks within an organization, and SYMANTEC databases of reported vulnerabilities – also historical, though worldwide (Chen, 2006). Both of these options rely on observed sample distributions and thus cannot be accurate predictors of future events, since they do not account for changing environments. Simply put, past events are not good predictors of the future –as is well documented in financial markets. Nevertheless, Monte Carlo analysis is a valuable tool for experienced financial analysts and presents high potential within the systems development framework.

Within financial risk management, the Monte Carlo technique is supplemented with Backward Recursion (decision-tree analysis), and Quasi-Random Sequences (interdependent simulations), etc. in order to model more complex factors (Jorion, 2009). Thus, there is an ample body of research to draw on if Monte Carlo is applied in practice to the systems security challenge; unfortunately these were not mentioned in the article. In contrast to the article, from my professional experience, unless an organization keeps a detailed database of system security vulnerabilities and costs, with a long enough lookback period for meaningful statistical analysis, it has to rely on external estimates, which may not be applicable to specific system model. In many cases ex-post cost analysis is not performed at all and the length of historical lookback period itself is problematic, given the changing information system environment -which makes any predictive statistical analyses doubtful at best. Such methods inherently depend on the skill and experience of the analyst, who needs to have a good understanding of model input estimates in order to gauge the confidence level of results. These challenges are common to all areas of risk analysis, from financial to organizational, including information systems security and design.

Conclusion

The article presents an application of financial risk management methodology to modeling information systems security risk. The proposed framework is well-grounded in established industry practices, as well as robust statistical models. Noel et al achieve a plausible decision-support metric for organizational systems security investment options, taking into account budget constraints and variable complexity. Such analysis would be a valuable complement within the systems development framework, as long as model sensitivity to quality of input variable estimates is kept in consideration. A comparison of Monte Carlo methodology results with existing System Security risk models would be interesting, as part of further research.

Works Cited

Chen, T. M. (2006). An Epidemiological View of Worms and Viruses. Annual Review of Communications, Vol 6 , 401-406.
Girao, P. S., Postolache, O., & Pereira, J. M. (2009). Data Fusion, Decision-Making, and Risk Analysis: Mathematical Tools and Techniques. Boston: Birkhauser.
Jorion, Phillipe; GARP (Global Association of Risk Professionals). (2009). Financial Risk Manager Handbook (5th ed.).
Hoboken, New Jersey: Wiley Finance.
Noel, S., Jajadia, S., Wang, L., & Singhal, A. (2010). Measuring Security Risk of Networks Using Attack Graphs. International Journal of Next-Generation Computing , 1 (1), 135-147.
Remenyi, D., Bannister, F., & Money, A. (2007). The Effective Measurement and Management of ICT Costs & Benefits. Oxford: CIMA Publishing.
Verissimo, P. E., Neves, N. F., & Correia, M. P. (2003). Architecting Dependable Systems. Heiderlag: Springer-Verlag Berlin.
Whitman, M. &. (2009). Principles of Information Security. Boston: Thompson Course Technology.

Svetlana Goubanova, CFA
Johns Hopkins University
svg@jhu.edu, goubanova@gmail.com