Understanding the Issues in Quantification and Management of Information Security Risks

Paper Category: Position Paper

This paper starts by giving an in-depth, technically sound, formal introduction to issues related to quantification of information security risks which has been considered as a grand research challenge. In this paper, we propose to map information security risks along three dimensions:- *Cost to Attack*, *Cost to Defend*, and *Timeline*. We are not aware of any published work which has proposed dimensionality based approach to information security risks.

We have treated security threat at finer level of details in terms of *Security Vector Elements*. We are currently investigating security vector element based approach in practical scenarios, and results are very encouraging. Our approach requires additional computational resources as it is evaluating information security risk at a fine grained level. But the results of fine grained analysis are more accurate, which overshadows the performance penalty in terms of computational cost. This paper works out on the ideas that we have proposed in our previous paper entitled "Cost Based Tradeoffs for Information Security Assurance"[1].

From the perspective of NSPW audience, we feel that section 6 focusing on directions for future research is most interesting. We have discussed in brief the various avenues in which research should progress so that substantial enhancements (developments) can be made in this field. We believe that, "*The more accurately we will be able to measure the risk, more efficiently will we be able to manage the risk*".

Justification for Inclusion

In this work we developed initial framework with which the problem of Quantification and Management of Information security risks can be addressed. This is a position paper that can invoke high level discussion and critique at the workshop. The management information system researchers have been taking a lead in addressing this problem. There needs to be a symbiotic and collaborative effort to incorporate core computer science information security principles to help in quantifying information security risks. As NSPW has always provided a platform for discussion of challenging and risky ideas, so we hope that our paper that focus on a grand research challenge will be included in NSPW-05.

---

[1] Ritesh Kumar Tiwari, Kamalakar Karlapalem, "Cost Based Tradeoffs for Information Security Assurance", Workshop on Economics of Information Security (WEIS-2005), Harvard University, MA. [June 2005]