When a system administrator configures a network so it is secure, he understands the users, data, services, servers and most importantly the intent — what is he trying to do. However, he does not understand well the mechanisms by which components interact and the details of each component. He could easily misconfigure the network so a hacker could steal confidential data. How does one enable the system administrator to securely configure the network with a limited understanding of its components and their interactions?

About hundred new security vulnerabilities are found per week. It becomes even more difficult to manage the security of a network installation in the presence of large number of security weaknesses in software under challenging time constraints. It is difficult to answer questions like Is this bug relevant on my network? What is the best workaround?

The costs of having a security vulnerability and taking actions to close it are high. Using a tool to help in these tasks will reduce errors, saves costs by eliminating redundant actions, streamlines actions by prioritizing between multiple bugs and actions. It also gives you a chance to plan ahead (“what if I find a problem with a web server?”). In future, we plan to extend our system to include the capability to estimate the risk associated with the current network profile (“The probability of the attack coming from this part of network is 80%.”).

MulVAL Technologies is targeting enterprise networks. IT security officers, penetration testers and security consultants would use the MulVAL tool to evaluate the security of their operational network. A system administrator will use the MulVAL tool to aid him in configuration. Developers would use the MulVAL tool to understand the effects of installing their software. Our alpha customers currently include the Computer Emergency Response Team, and the U.S. Department of Energy.

Go-To-Market Strategies The company will sell the tool directly to individual enterprise system administrators. The company will sell this software by partnering with enterprise network infrastructure management tool vendors.

Technology At MulVAL Technologies, we developed the fundamental insight that each component of a network has a very well defined deterministic behavior. By understanding the behavior of each component, the tool can understand how different components interact. By automatically incorporating security advisories using off-the-shelf tools, our expert system determines the network wide impact of all security holes on the network. Previous approaches to this problem have drawbacks in one or more of the following: end-to-end automation, understanding multiple operating systems, efficiency, system architecture. We have filed patents on our technology.

Status/Requirements MulVAL is in the process of creating the initial team. It is looking for a person with business experience in starting and running early stage companies. It is looking for someone with an advanced understanding of computer security industry. MulVAL is currently converting research into first version of the product. It is developing other technologies supported by a government grant.

MulVAL Technologies is based on research conducted at the Princeton University. The MulVAL framework that understands the semantics of different components, takes inputs from off-the-shelf vulnerability scanners and automatically finds ways which a hacker could compromise the network. This framework has been used to find serious security holes on the Princeton University campus network and also in software from major vendors.