

Title: Towards an Attack-Resistant Desktop

We propose a system intended to provide high availability through redundant system components and rapid recovery against viruses, worms, problematic system updates, and any other adverse system changes. Many systems are vulnerable because they do not run the latest virus definitions or security patches and even systems that are fully patched are susceptible to zero day attacks. Also, system or application updates can break other software packages or cause the system to become unstable. Our approach uses four key techniques: (1) isolate user data on a file system virtual machine and allow rollback if an attack has introduced modifications or corruption, (2) separate applications from each other by running them in virtual machine appliances and allow rollback if an attack or system instability is detected, (3) use standard network-based intrusion detection systems to detect incoming attacks and also suspicious outgoing activity, and finally (4) add a novel approach to file system intrusion detection by creating application-specific data protection contracts. This talk will discuss the design of our system and suggest possible implementation strategies.