Minimizing Attack Vectors in Computer Systems by Evolving Access Control Matrices

Benjamin Daniels

ABSTRACT
A method is proposed which offers a strategy to design computer architectures, including kernel and network architectures, which will be hardened from cyberattacks. A whitelist is used within an access control matrix to restrict malware, and also to restrict subsystem interaction to what is required for functionality down to the object level, severely restricting system exploitability. Machine learning is used to evolve the composition of and relationships between system objects, with respect to their atomic functions, so as to minimize the number of paths an attacker may take to compromise protected resources of the system. The final set of vulnerable paths are identifiable, and may therefore be thoroughly vetted against exploitable flaws, or further hardened by other means. Finally, user alerts are used to add a final level of security in a way which maximizes their effectiveness through footprint restriction, thereby alleviating user desensitization.