Strategies for network security.

Summary: Security of networks has become an increasingly important issue in the highly connected world. Security depends on attacks. Typical attacks include both cascading failure of virus spreading and of information propagation and physical attacks of removal of nodes or edges. Numerous experiments have shown that none of the existing models construct secure networks, and that the universal properties of power law and small world phenomenon of networks seem unavoidable obstacles for security of networks against attacks. Here, we propose a new strategy of attacks, the attack of rules of evolution of networks. By using the strategy, we proposed a new model of networks which generates provably secure networks. It was shown both analytically and numerically that the best strategy is to attack on the rules of the evolution of networks, that the second best strategy is the attack by cascading failure models, that the third best strategy is the physical attack of removal of nodes or edges, and that the least desirable strategy is the physical attack of deleting structures of the networks. The results characterize and classify the strategies for network security, providing a foundation for a security theory of networks. Equally important, our results demonstrate that security can be achieved provably by structures of networks, that there is a tradeoff between the roles of structures and of thresholds in security engineering, and that power law and small world property are never obstacles of security of networks. Our model explores a number of new principles of networks, including some topological principles, probabilistic principles, and combinatorial principles. The new principles build the foundation for new strategies for enhancing security of networks, and for new protocols of communications and security of the Internet and computer networks etc. We anticipate that our theory can be used in analyzing security of real systems in economy, society and technology.

Keywords: complex networks; security of networks; strategy for network security; cascading failure; model of networks
doi:10.1007/s11432-014-5182-9