CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Modeling and Simulating the Cost and Impact of Cyber Attacks : Malware Threats

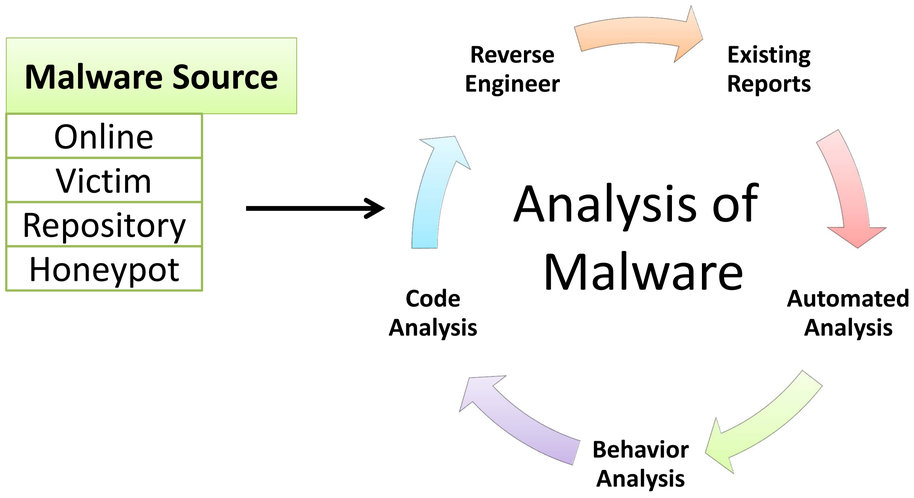
Cory Q. Nguyen, Dr. J. Eric Dietz
Purdue Homeland Security Institute

Overview

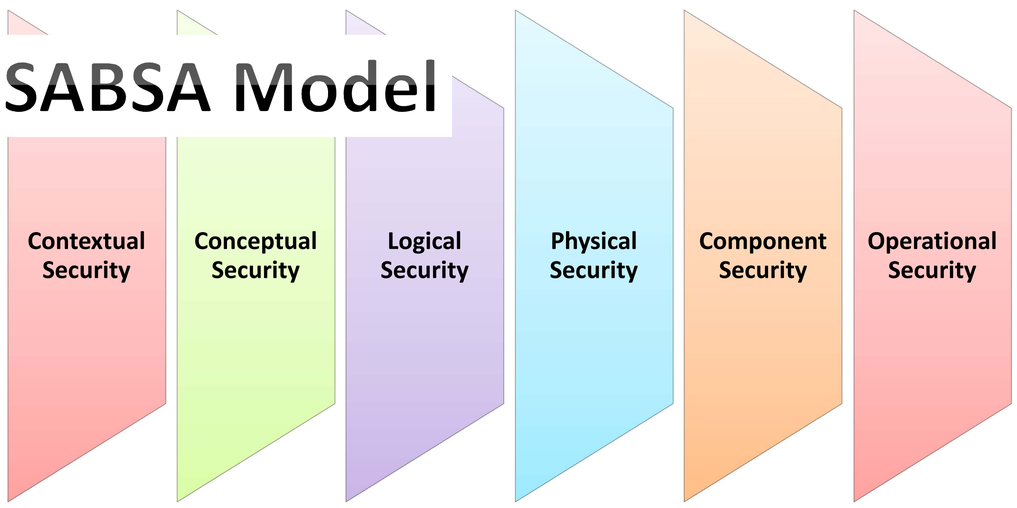
This study's goal is to model and simulate the impact and cost a malware threat has on an organizations and its subsidiaries. The model's purpose is to measure both direct and indirect cost and impact of a given malware. Currently, a model of campus is being developed.

Given the ability to visualize and reasonably assess the impact of a given malware and the potential cost incurred, organizations can have a better grasp of its current ability to prevent, address, and mitigate future potential threats. Additionally, it would have a more clearer picture of future implementations and action items needed to manage the risk responsibly. Simply, with the ability to model and simulate a given malware threat of a specific organization gives knowledge and insight to develop a thorough and reliable risk management system.

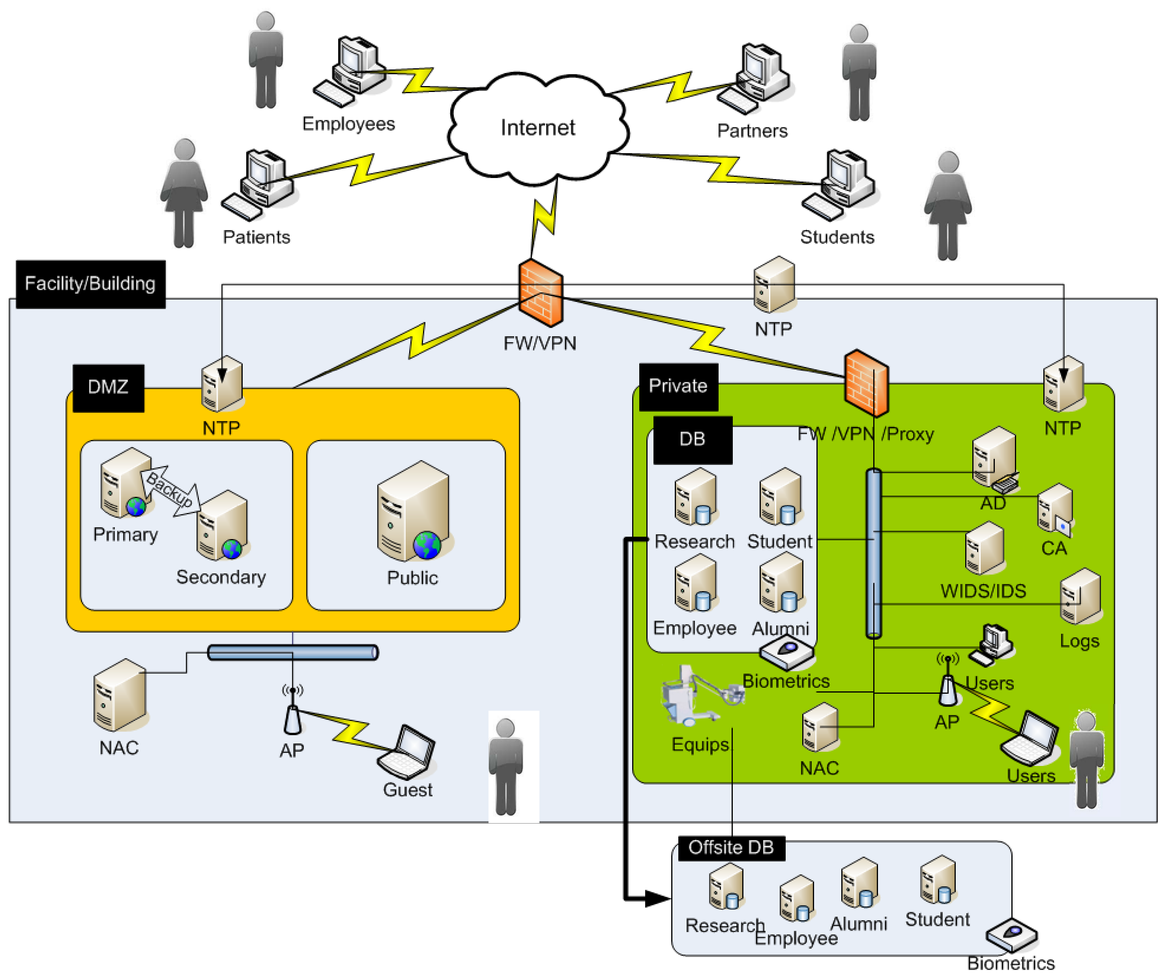
Step 1: Malware Knowledge



Step 2: Establish Security Architecture of Organization



Step 3: Create Model of Security Architecture of an Organization/Campus



i.e.: Infrastructure of a Campus Organization

Step 4: Run Simulation w/ Particular Malware Specification