

Network incidents anticipation poster abstract

Elie Busztein

July 13, 2007

Evaluating network resilience to incidents such as hardware failures and intrusions is important for network security. A key issue in this evaluation is to evaluate the collateral effect of an incident on the network. For example a classical collateral effect of a DOS on company DNS servers is that the company web site is merely not reachable because web browsers are not able to perform DNS resolution.

A way to address this issue is to analyze the network to ensure that there is no incidents scenario possible for a given service. An incident scenario can be intuitively defined as a set of vulnerabilities or failures and their collateral effect used as as step-stones to disable or compromise a given service.

Our work consist of the theory and the set of software used to prove automatically that a network service is resilient to incidents. If the service is proved not resilient, then a incident scenario is as counter example. Our framework, called NetQi, has three main specificity. One it takes into account the dependencies between network services to evaluate the collateral effects. Two it models administrator dynamic response to incidents, such as patching or firewalling. Three it takes time into account which allows to model that launching an exploit is faster than patching a service for instance. To accomplish so our framework is based on a variant of TATL (Timed Alternating-Time Temporal Logic) we have created for this purpose. The framework uses two software. The first passively monitors the network to extract topological information and infers services dependencies by the mean of statistics and Ngram. The second uses network information to build the model and verify the resilience.

Our framework, introduces a new type of tool designed to help the administrator to improve the resilience of its network against incidents.