

form and detail can be made therein without departing from the spirit and scope. In fact, after reading the above description, it will be apparent to one skilled in the relevant art(s) how to implement alternative embodiments. Thus, the present embodiments should not be limited by any of the above described exemplary embodiments. In particular, it should be noted that, for example purposes, the above explanation has focused on the example(s) analyzing attack graphs for a computer network. However, one skilled in the art will recognize that embodiments of the invention could be constructed and used to analyze any type of network. For example, one could use embodiments to analyze attack graphs for road systems. In this example, it may be useful to analyze attacks on a geographical location in an attempt to decrease the likelihood of future attacks on that geographical location.

[0123] In addition, it should be understood that any figures which highlight the functionality and advantages, are presented for example purposes only. The disclosed architecture is sufficiently flexible and configurable, such that it may be utilized in ways other than that shown. For example, the steps listed in any flowchart may be re-ordered or only optionally used in some embodiments.

[0124] Further, the purpose of the Abstract of the Disclosure is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract of the Disclosure is not intended to be limiting as to the scope in any way.

[0125] Finally, it is the applicant's intent that only claims that include the express language "means for" or "step for" be interpreted under 35 U.S.C. 112, paragraph 6. Claims that do not expressly include the phrase "means for" or "step for" are not to be interpreted under 35 U.S.C. 112, paragraph 6.

What is claimed is:

1) A system for analyzing attack graphs, comprising modules residing on at least one tangible computer readable medium containing a set of computer readable instructions that are executable by one or more processors, the modules comprising:

- a) a network configuration information input module configured to input network configuration information that describes the configuration of a network, at least part of the network configuration information describing at least part of the physical structure of the network, the network configuration information including at least one of the following:
  - i) host information;
  - ii) host configuration information;
  - iii) application information;
  - iv) network service information; or
  - v) operating system information; or
  - vi) a combination of the above;
- b) a domain knowledge input module configured to input domain knowledge for the network, the domain knowledge including knowledge about at least one exploit;

- c) a network configuration information storage module configured to store the network configuration information in at least one network database table;
- d) a domain knowledge storage module configured to store the domain knowledge in at least one exploit database table, the domain knowledge including exploit information; and
- e) a result generation module configured to generate a result using the network database table and exploit database table in response to a query to a database management system, the result including at least one of the following:
  - i) a metric;
  - ii) an attack path;
  - iii) part of an attack path;
  - iv) a collection of paths;
  - v) an exploit;
  - vi) a condition-exploit pair;
  - vii) an exploit-condition pair; or
  - viii) a table that describes an attack graph; or
  - ix) a combination of the above; and

wherein the network is reconfigured using attack information learned from the result.

- 2) A system for analyzing attack graphs, comprising:
  - a) a network configuration information input module configured to input network configuration information that describes the configuration of a network;
  - b) a domain knowledge input module configured to input domain knowledge for the network, the domain knowledge including knowledge about at least one exploit;
  - c) a network configuration information storage module configured to store the network configuration information in a network database table;
  - d) a domain knowledge storage module configured to store the domain knowledge in an exploit database table; and
  - e) a result generation module configured to generate a result describing at least part of a network attack using the network database table and exploit database table.
- 3) The system according to claim 2, wherein the network configuration information input module, the domain knowledge input module, the network configuration information storage module, the domain knowledge storage module, and the result generation module reside on at least one tangible computer readable medium containing a set of computer readable instructions that are executable by one or more processors.
- 4) The system according to claim 2, wherein the network configuration information includes host information and host configuration information.
- 5) The system according to claim 2, wherein at least part of the network configuration information describes at least part of the physical structure of the network.
- 6) The system according to claim 2, wherein the network configuration information includes application information.