PHD THESIS ABSTRACT

EFFECTIVE MANAGEMENT SUPPORT ON NETWORK AND COMMUNICATIONS SECURITY:

IDENTIFYING AND RESPONDING TO SECURITY INCIDENTS

Dimitrios G. Patsos

This work approaches a series of issues related to security incident identification and response, as well as the capability of information technology and communication systems security through effective management and technical mechanisms.

We initially propose a taxonomy that includes the main concepts of the research area, by defining relative terminology and examining the interrelationships between the basic terms.

We discuss in detail the main issues of incident identification and response within a corporate environment, while we propose a management framework based on academic and applied research, as well as international best practices, security standards and technical implementations. Furthermore, we propose a structured methodology and discuss in detail every distinct phase of this methodology.

Furthermore, we approach the technical issues related to incident identification and response, while we propose and discuss in detail the requirements of an incident identification and response system.

We then propose and present the Incident Response Intelligence System - IRIS, a system performing topological analysis to vulnerabilities identified by associated tools, scoring their significance with a standardized method, while also correlates the relative exploit code and defines the corresponding intrusion detection signatures for these vulnerabilities.

Finally, we evaluate IRIS implementation against the design specifications, present and discuss a series of experimental data and we evaluate IRIS functionality in real-world scenarios.